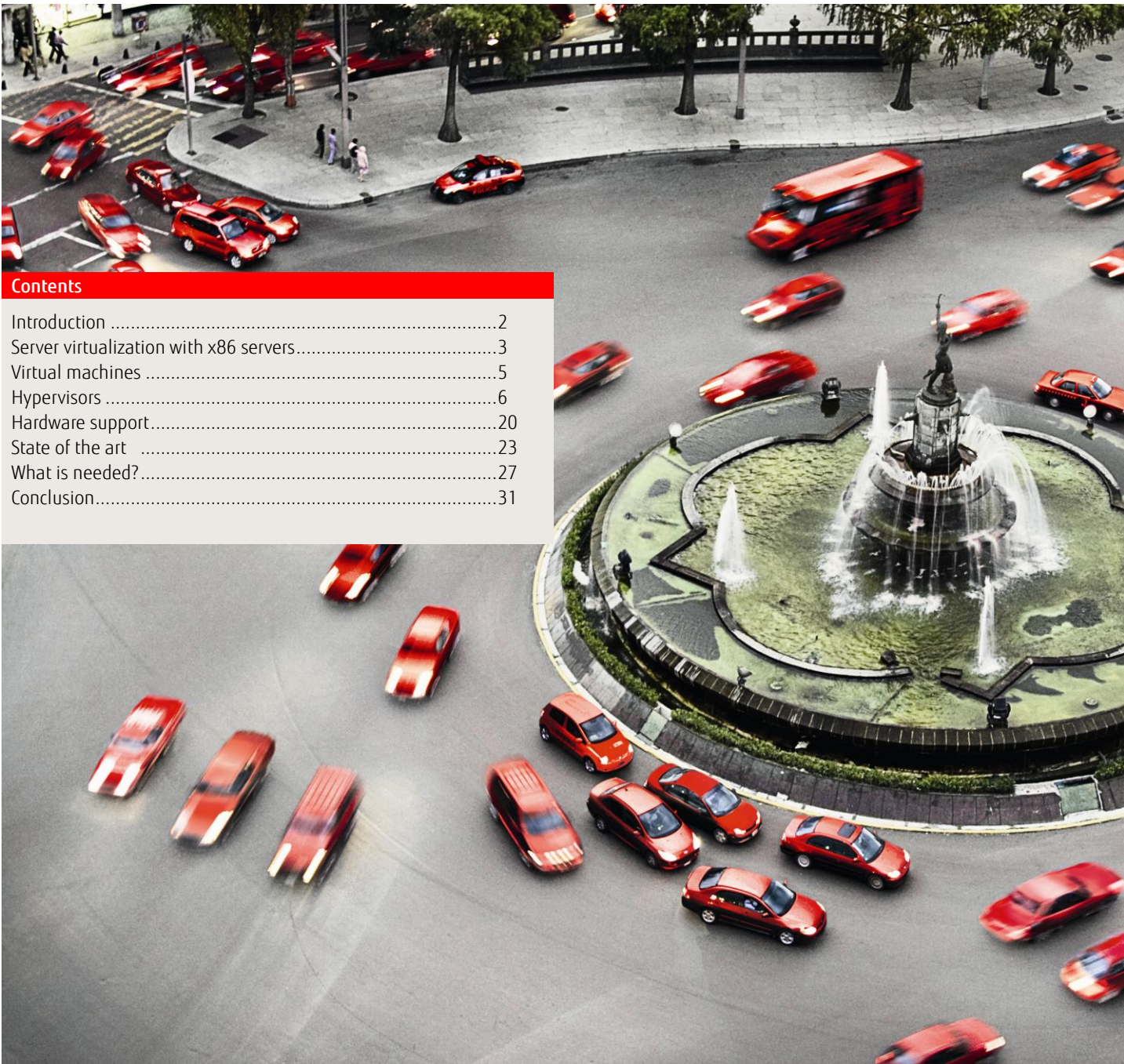


White paper

Virtualization at Fujitsu

This whitepaper examines the various virtualization technologies and shows the range of ICT infrastructure layers where they are applied. It also shows how Fujitsu incorporates these technologies into end-to-end solutions as an essential part of its Dynamic Infrastructures strategy.



Contents

Introduction	2
Server virtualization with x86 servers.....	3
Virtual machines	5
Hypervisors	6
Hardware support.....	20
State of the art	23
What is needed?	27
Conclusion.....	31

Introduction

What is virtualization?

Broadly speaking, virtualization in an information and communication technology (ICT) environment is about breaking the dependencies between the various layers in the infrastructure. Introducing a virtualization layer enables abstraction from the complexity of the underlying layers. However while it hides the complexity it also mediates access to it, allowing the creation of virtual resources that can be mapped to the underlying physical resources. This definition is applicable at any level where virtualization is applied.

Virtualization is not new

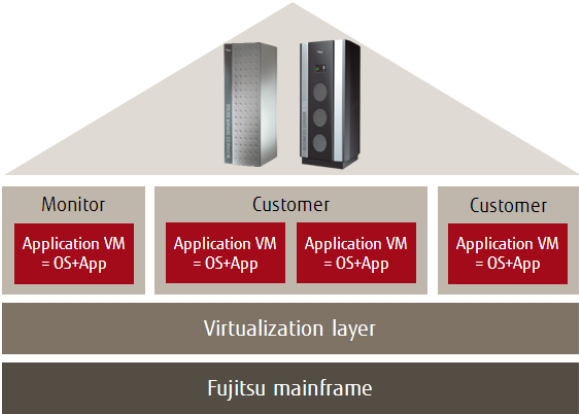
Virtualization, introduced more than 30 years ago with mainframe systems, initially pursued two basic objectives:

- With server hardware extremely expensive at the time, it needed to be fully utilized to gain maximum cost benefit. Server virtualization enabled grouping of the various operating system (OS) instances on the same physical hardware system. That significantly improved flexibility and capacity utilization.
- By separation of the application requirements from the restrictions of the physical hardware and software infrastructure layers, virtualization enabled further development of new technologies, without impact on the existing software infrastructure.

The technology developed at that time corresponds very closely to the current approach to server virtualization using modern day hypervisor technology.

Server virtualization is rooted in mature mainframe technology

Fujitsu was one of the virtualization pioneers, and has decades of experience in providing and managing virtual machine infrastructures. Fujitsu GlobalServer and BS2000 mainframes are perfect examples of continuity and long-term investment protection in mission-critical datacenter environments brought about by virtualization. This ongoing development has allowed resource allocation to occur dynamically at a very granular level. It has also meant considerable reductions in energy consumption, space and administrative effort. In addition, it has achieved high availability in a cost effective manner, with services made ready much faster. A virtualized approach also enables parallel operation of production, test, and development systems allowing both pre- and post-production systems to exist on the same hardware.



Today the approach to virtualization and the levels at which it is applied are more diverse. The following diagram shows the various infrastructure levels of virtualization deployment and the solutions that are frequently used.

Application abstractions	Reg. DLL Folder EXE	Microsoft SoftGrid, Altiris Software Virtualization Solution, Ardenne, SAP, Oracle...
Desktop abstractions	App. DLL Thin C. RDP	VMware View, Citrix XenDesktop Server, ...
Container abstractions	App Thread JVM Proc.	Solaris Zones, SWSoft, Virtuozzo/OpenVZ, Java EE...
OS-based VM abstractions	vOS OS	VMware (GSX) Server, Microsoft Virtual Server, KVM...
Hypervisor-based VM abstractions	vCPU vHDD	VMware ESX Server, Xen, Microsoft Hyper-V
Physical abstractions	HT Core I/O	Intel Virtualization Technology (VT), AMD Virtualization (AMD-V)...
Server I/O abstractions	vEth vHBA	Fujitsu SV-VIOM, Fujitsu ServerView RCVE
Network abstractions	vSwitch TCP vLAN	Cisco, Brocade...
Storage abstractions	FS LUN Disk Tape	Fujitsu ETERNUS CS, Fujitsu ETERNUS DX, EMC, NetApp, Veritas, Brocade, Microsoft...

The wide range of virtualization solutions however means that a key task of ICT managers is identification of the right technology for each specific requirement, and integration of that into the ICT infrastructure. However, the diagram clearly shows that no single virtualization layer will likely meet all requirements in a state-of-the-art dynamic infrastructure. Instead, a combination of the various technologies is required to create an ideal customer-specific solution.

This white paper discusses the best-known technologies, shows their advantages and describes their connections with other layers and solutions. It presents the technologies that Fujitsu uses, as well as those it has developed in-house, to offer each customer a consistent, end-to-end, virtualization solution.

Server virtualization with x86 servers

No other server architecture has gained in importance over the past decade as much as x86-based server platforms. The complete Fujitsu PRIMERGY product family is the embodiment of this form of architecture, and based today on virtualization support in processor technology. The rapid pace of this technology results in an unprecedented ICT price/performance ratio. In fact, other components have trouble keeping up with the speed at which the hardware is developing. That results in special requirements for this platform, which are tackled by virtualization.

The traditional x86 platform approach

The architecture of a traditional industry standard server consists of three important layers.

- First is the hardware layer, which is a set of different devices and compute resources.
- Second is the OS layer, which has overall control of hardware operation. It is responsible for managing the hardware resources and sharing them among the different tasks, based on priorities.
- Third is the applications/services layer, which uses the OS as an interface to access the required hardware resources.

In this traditional platform approach, each configuration layer is tightly coupled to each preceding (or lower) layer. As a result, hardware and software lifecycles are strongly dependent on each other. This means for example, a legacy application that runs on an OS not supported by new hardware cannot upgrade to that new hardware. As hardware changes regularly, this becomes a serious issue.

Due to historical reasons, OS resource management is not very efficient and applications can interfere with each other over joint use of particular resources. This can lead to servers, sized and installed for peak loads, running only a single application. This resulting over-provisioning of system resources leads to correspondingly poor server utilization. Poor server utilization, in its turn, leads on to an explosion in server numbers, high energy consumption, additional heat generation, expansive floor-space requirements, and of course higher expense on maintenance and support. Likewise, scalability is limited dynamically and high availability becomes difficult and expensive to implement.

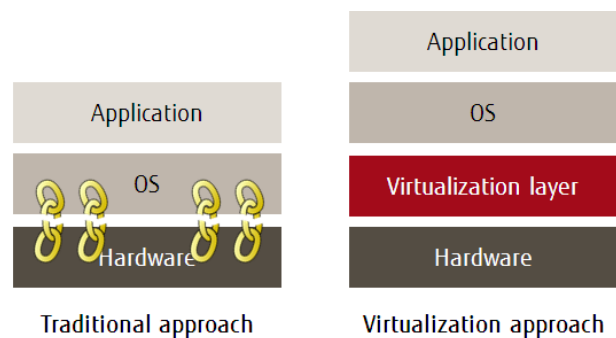
The overall result is management complexity and low efficiency, with considerable effort needed to deploy new services; i.e. the time required to respond to changes in business is too long.

The traditional platform approach therefore becomes synonymous with a high Total Cost of Ownership (TCO).

x86 platform virtualization

To overcome the traditional challenges created by the strong dependencies between hardware and OS, a decoupling must occur. The use of hypervisor or "server virtualization" technology achieves this.

By definition, server virtualization means hiding the server resources, including the number and the identity of each physical server, processor, and OS, from the end users. In particular, applications and services now operate independent of the dedicated hardware resources. This enables more flexible control of both hardware and software resources, and improves the value proposition across a wide range of ICT requirements. According to a range of studies, virtualization will be a pervasive and important trend in servers through 2014.



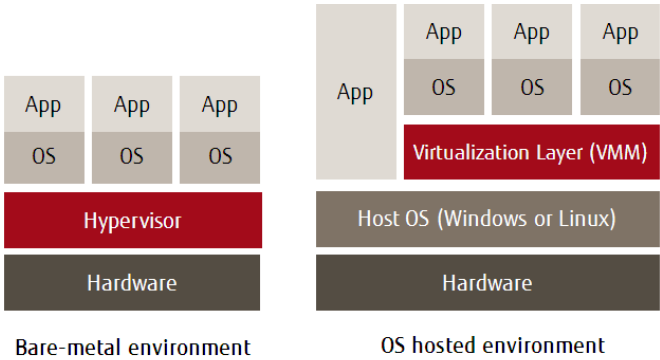
Hypervisor technology lets multiple instances of an OS and associated applications run on the same physical hardware system. It also enables the consolidation of large numbers of under-utilized physical servers onto fewer well-utilized servers. Virtualization creates independence between the software and hardware layers and becomes the foundation for new operating processes.

In the past, the ability to run older OS versions on the latest hardware was one key motivation for deploying hypervisor technology. Now customers also expect further benefits from server virtualization; in particular greater agility, higher availability and lower operating costs.

Virtual machines in OS hosted environments

Some virtualization technology is used less with today's x86 servers. OS hosted environments are an example. Here the virtualization layer sits on top of the host OS, and is just one of the many features of the physical server's OS. In this case, the virtualization layer has the status as any other application running on the hardware and OS. It also exclusively uses the device drivers and resource management of the host OS. Examples are VMware Server and Microsoft Virtual Server.

The virtual machine concept in OS hosted environments came into being at the early stage of server virtualization. One of the main areas of application was the ability to run different development and test systems on the same hardware. Today this is only relevant in small system environments.



Customer expectations of the virtual machine concept

When it comes to the question of what customers expect from the virtual machine concept, we have to distinguish between large enterprises and mid-sized companies. While the overall perspective of both can appear the same, their priorities are often different. With large enterprises the top five priorities are as follows:

- Consolidation: Which provides the opportunity for dramatic capital equipment cost savings.
- Virtualization: As an enabler in reducing the administrative burden of loading and configuring the endless numbers of new servers arriving on the loading dock.
- Operational agility: The ability to move workloads from one server to another as changes demand, with reduced administrative effort.
- Freedom of choice: Virtualization makes it easier to accommodate a mix of vendors and server models, within the datacenter.
- Protection: Virtualization simplifies disaster recovery - but only with x86 platforms.

However due to the heterogeneous nature of most large enterprise ICT infrastructures, replication for disaster protection tends to be complex. That is why protection has the lowest priority in their top five. In general, it is fair to say, large enterprises tend to focus on the cost savings associated with virtualization.

Mid-sized businesses have the same expectations, but their top five implementation priorities are different:

- Consolidation: This is number one here too, but the level of savings is lower due to the smaller server deployment scale.
- Protection: Number five with large enterprises, it rises to number two with mid-sized businesses. Here virtualization and low-cost Storage Area Network (SAN) are often combined. This can significantly reduce the cost and complexity of implementing disaster recovery.
- Deployment: Most mid-sized businesses have limited administrative resources. Virtualization helps reduce administrative effort and increases speed of deployment.
- Freedom of choice: Virtualization allows purchases based on competitive pricing without worrying about the overheads of supporting multiple vendors.
- Operational agility: Here virtualization helps in adapting server resources to changes in workload demands. While not at the same level as with large enterprises, implementing new services at branch offices, for example, becomes much easier.

Overall, mid-sized businesses, while also driven by the promise of consolidation and cost savings, see virtualization as an opportunity to introduce solutions that would otherwise be difficult and expensive to deploy.

Virtual machines

By definition, a virtual machine is a software-driven implementation of a computer. One that executes programs in an identical way to a physical machine but which runs as an isolated environment as part of the physical computer. A virtual machine is also described as a guest, with the physical computer as the host. As numbers of virtual machines can run on a single physical machine, the physical machine will appear to users to behave like many servers.

Server virtualization tricks the virtual machine into only seeing the same virtual hardware (CPU, memory and I/O devices) regardless of the overall underlying equipment in the physical machine.

Key features

Four key features characterize the virtual machine concept.

First, virtual machines are fully isolated from each other. Isolation is essential to ensure process availability and maintain security. If for instance a virtual machine fails ("blue screen"), there must be no impact on other virtual machines running on the same physical hardware.

Second, the overall physical server hardware is partitioned into several virtual machines, each running its own (guest) OS. Each guest OS may be quite different. Hardware resources, such as CPU, main memory or I/O devices, are shared among the virtual machines. A technique called encapsulation saves the status of each virtual machine as a file. Simply by copying this file, the virtual machine is transferred quickly and easily from one physical environment to another.

Third, with the hypervisor situated between the software stack (containing the OS and the application) and the server hardware, software and hardware can operate completely independently. This enables running of legacy applications on the latest hardware technology, even though the OS needed to run the application does not support the necessary drivers on the new physical hardware. The hypervisor acts as an intermediary and ensures the investment protection of legacy applications.

Fourth, all virtual machines are contained in a common file system, e.g. VMFS (Virtual Machine File System). This permits the building of failover clusters between virtual machines. This is much more affordable than clustering using physical servers; which are traditionally expensive, complex and difficult to manage.

Case studies

Major university in Tokyo

With three separate campuses in the greater Tokyo area, this science and technology university was seeking a way to reduce their total cost of ownership of ICT equipment. The existing UNIX servers at each location required separate administration as well as local Network Attached Storage (NAS). Introduction of 500 Mbps inter-campus transmission speeds paved the way for a more consolidated approach. The move to on-demand remote class work has also put pressure on the inflexibility of the existing systems. Initially they envisaged a virtual machine environment at each campus. However, with the new communications backbone this quickly developed into a centralization plan.

Extensive testing and evaluation lead to the adoption of a Linux environment based on Fujitsu PRIMERGY rack servers and VMware plus data consolidation in a Storage Area Network (SAN) based on Fujitsu ETERNUS DX storage, with VMware vMotion for data migration. The result was of the migration of 20 UNIX servers onto just 12 Red Hat Linux servers. In addition, the university discovered that the new centralized environment had the capacity to handle 80 plus virtual machines. This would also support their future growth, with fast deployment and no disruption to existing services. The success of this work and the enhanced fault tolerance of the new infrastructure have drawn great attention from other major private universities.

Server virtualization at Finish investment bank

This Finnish investment bank runs its own in-house developed applications at brokerage offices around the world. However, in the past, based on their perception of the best local support, each of the local offices procured the required hardware independently. The result was a rather heterogeneous server landscape. This caused major problems and high administration costs, particularly when new applications needed delivery for testing and local implementation.

Now using virtualization technology, the Bank performs quality assurance and testing at their headquarters. This means a significant saving in development and system assurance costs. Deployment also occurs easily and rapidly, as headquarters staff simply copies the two binary files of the tested virtual machines, and remotely deliver them to the target systems, wherever they are worldwide. This is possible because virtualization separates the requirements of the applications from the underlying hardware resources. New services are deployable within minutes and if a disaster occurs, fast recovery using the system backup copies is quick and simple. Now everything works with minimum administration effort.

Hypervisors

General characteristics

There was for a long-time detailed debate on the best type of hypervisor architecture. Which created the lowest overhead, and what virtualization method was the most efficient?

"Para-virtualization", "full virtualization", "trap and emulate" and "binary translation" (see page 21) are some of the buzz words used in this connection. However once standard processor technology started to support virtualization, the debate was pushed to the background. Most hypervisors now use these "hardware assist" processor interfaces and all achieve comparable performance. Para-virtualization, where some time-critical functions are performed on the host rather than in the virtual machine, is now only used in exceptional cases; in particular, where the hypervisor vendor also has unrestricted access to the OS.

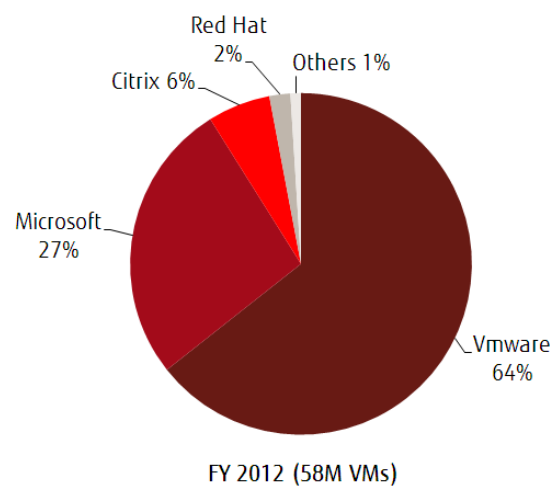
In addition to this standardization of virtualization methods, all vendors offer functions that result in higher availability and agility, as well as efficient management of the virtual environment. All hypervisor vendors offer a special management suite for virtualization. Each offering differs in terms of its management coverage and end-to-end solutions and this has become the prime criteria for choosing a suitable hypervisor. As a result, the basic hypervisor has become a commodity component. So, in comparing the price of different products, it is essential to analyze the product structure and the range of associated functions closely, to obtain truly comparable results.

Note that major ISVs now offer their products as appliances, i.e. the application ships as part of the virtual machine and not in conventional installation format. Consequently, the application is independent of the type of server it runs on. This reduces the time and effort ISVs need to spend on Q&A. However, it can result in end customers using more than one hypervisor. To minimize the complexity this involves, vendors are working on standardizing VM formats (for example Microsoft and Citrix) enabling virtual machines of a specific hypervisor to run on another hypervisor, at no cost or effort. This feature is also important when choosing a suitable hypervisor.

Virtualization technology in the x86 market started around the year 2000, with client and server offerings from VMware. The initial technology was based on software emulation (binary translation). Then in 2004/2005, processor vendors AMD and Intel implemented basic software aware hypervisor functions in the hardware layer. This meant CPU and memory functions, previously handled in the software stack, now became available to hypervisor vendors as a "function call". This was the catalyst for other hypervisor vendors to enter the market with new offerings based on the "hardware assist" technology of the processor vendors.

Market relevance

Today over 20 hypervisors are available in the market, but the direction is towards a few dominant hypervisor vendors. It is for this reason that Fujitsu primarily focuses on a select few hypervisors for its consolidation solutions. The following graphic from the Gartner research company, shows the projected market share for virtualization vendors in 2012, by number of VMs deployed.



Note: The sequence of product explanations that follow in the next section is not in exact market share sequence. Instead, it follows the chronological sequence of product development and dependency.

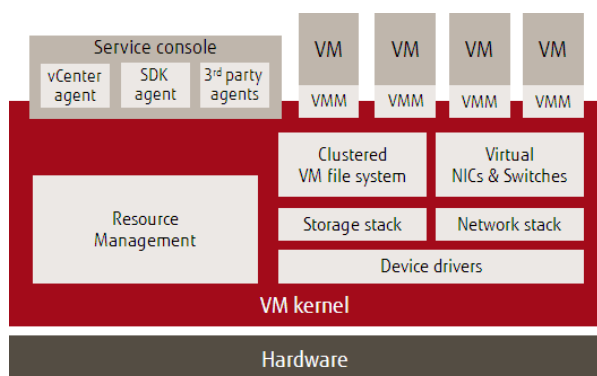
1. VMware vSphere

VMware has been an influential force in shaping server virtualization over the past decade. VMware's virtualization technology began with the PC (GSX). For the first time, multiple OS could run on the same PC allowing more flexible test environments. It was not long before this method was also used with servers.

As a result, the focus shifted to server consolidation and the possibility of running aging Windows NT4 environments on the latest hardware. With its vCenter management software, VMware set new standards in the management of virtualized environments. High availability (HA), load balancing within vSphere server farms, distributed resource scheduling (DRS), and above all vMotion, which lets virtual machines move during operation from one physical instance of the vSphere farm to another, were all pioneering developments. They also had a lasting influence on the planning of other vendors. The next step was fault tolerance (FT) which enables continuous operation by mirroring virtual machines on another vSphere host. Interaction between layers has also improved with many built-in Application Programming Interfaces (APIs). Security software vendors, Storage vendors and Network vendors (Cisco Nexus 1000), can now use these APIs (VMsafe, vShield) to deliver more highly optimized infrastructures.

Overview of the vSphere hypervisor

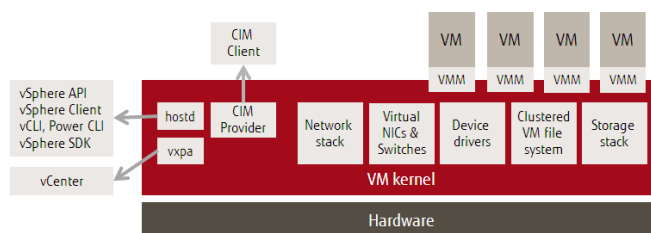
The current "classic" VMware architecture looks like this:



The VMware vSphere hypervisor runs directly on the hardware layer and acts as an independent OS. The kernel takes care of all of the following:

- Management of the VMs
- Separation of the VMs from each other
- Efficient distribution of resources between VMs in line with administrator requests
- Mapping of machine instructions issued in a VM
- Mapping of I/O jobs

The overall size (2GB) of the classic main version is due to the Linux subsystem. The subsystem enables the installation of agents to manage the underlying hardware. It also includes interfaces for management of the hypervisor. VMware intends to phase out this architecture in 2011 and reduce the hypervisor back to its pure kernel stack, with special interfaces for management. The future embedded VMware architecture looks like this:



VMware developed this kernel, with its impressive lean design requiring just 70MB, in-house. The results will be:

- No further need to support the Linux subsystem
- Greater security and protection from external attacks
- Easier implementation on OEM hardware with cost and efficiency benefits for users.

Info box

Common Information Model (CIM)

With the removal of the subsystem in which agents can run, a new interface is required. This now becomes the task of each hardware vendor using the new Common Information Model (CIM) Interface. CIM is an open standard that defines how computing resources are represented and managed. It enables a new framework for agent-less, standards-based, monitoring of hardware resources for the vSphere hypervisor. This framework consists of a CIM object manager, otherwise called a CIM broker, and a set of CIM providers. Each hardware vendor will need to create specific CIM providers for their hardware.

CIM providers are mechanisms that enable management access to device drivers and underlying hardware. In fact hardware vendors (both server manufacturers and specific hardware device vendors), will now have the flexibility to write CIM providers that best monitor and manage their particular devices. VMware is also writing providers that implement monitoring of server hardware, storage infrastructure, and virtualization-specific resources. These providers run inside the vSphere system and are designed to be extremely lightweight and focused on specific management tasks. The CIM object manager in vSphere hypervisor has a standard interface. Developers use this to plug-in new providers. However, the providers must be packaged with the system image, and cannot be installed at run time. The CIM broker takes information from each CIM provider and presents it to the outside world via standard APIs, including WS-Management

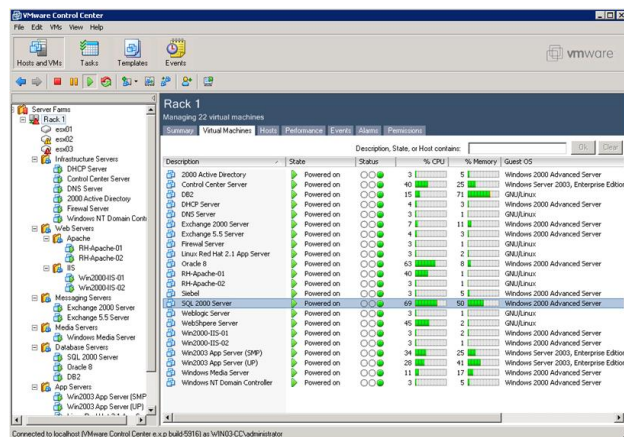
The lean kernel design, in particular, distinguishes VMware vSphere from other hypervisor architectures. VMware no longer needs the support of another operating system instance to handle its tasks. This makes it independent of any restrictions that may occur with such instances.

However, interaction with other OS instances (see section on Citrix XenServer and Microsoft Hyper-V) can have advantages, in particular with I/O handling. VMware vSphere hypervisor is the connecting link between the VMs and the underlying hardware. Each VM only “sees” the formally supported hardware (SCSI disks, Network Interface Cards (NICs), processors and storage; however, this does not always correspond to all existing hardware the hypervisor has to serve. To address all hardware from the hypervisor, drivers exist for most common hardware components. However, caution is required if special hardware components are needed for an application (e.g. security dongles, ISDN cards, special graphics support, etc.). It is then necessary to check on a case-by-case basis whether VMware supports the relevant drivers. Manufacturers of each special hardware component must ensure they certify with VMware for the servers in question. Manufacturers not on the VMware Hardware Compatibility List (HCL) cannot expect support from VMware in the event of an error.

VMware management

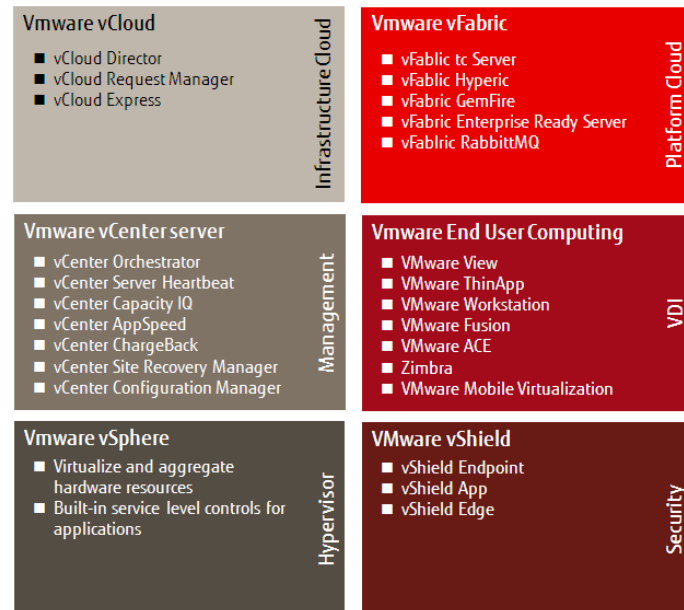
As mentioned at the outset, management of virtualized infrastructures is a core component in every hypervisor scenario. The following shows the core functions of VMware vCenter:

- Centralized management interface
- VM provisioning with templates
- Performance monitoring
- Secure access control
- SDK (Software Development Kit) for automation



VMware vCenter focuses on managing the virtual machines (VMs). In line with VMware’s philosophy, real server instances no longer play a major role. The real instance, the VMware server, is viewed as part of the server farm. The resources, the server contributes to the farm, are comprehensively administered by the relevant management layers, and divided among the VMs as specified. Individual servers no longer play a role in this distribution. VMware vCenter allows a new server to be included in a server farm with very little effort. It also enables simple replacement of servers that have failed due to a hardware fault. However, VMware vCenter does not enable the provisioning of substitute physical servers. This requires the addition of automated processes or products, such as Fujitsu ServerView Resource Coordinator VE (See separate section in this white paper.)

VMware provides a comprehensive range of proven technologies that enable end-to-end solutions. VMware has a wide ranging and powerful stack of solutions including, site recovery manager, fault tolerance, data recovery, thin provisioning, distributed virtual switching and dynamic power management. Certainly, VMware has the broadest portfolio of solutions of any hypervisor.



VM migration technology

One great advantage of server virtualization is the ease of handling virtual machines. Virtual machines are handled as files in a common cluster file system. This independence from the underlying server hardware makes it easy to (re)start a virtual machine on every virtualized host system running the same hypervisor.

Agility is the next benefit, in particular this covers the ability to move a virtual machine from one server to another while it is running. All hypervisor vendors deliver this functionality under various names including, vMotion (VMware), XenMotion (Citrix) and Live Migration (Microsoft). Here we will use a vMotion example, but the technology and functions of each are very similar.

VMware vMotion

Three underlying technologies enable the live migration of a virtual machine from one physical server to another.

First, the entire virtual machine is encapsulated in a set of files on shared storage (Fibre Channel or iSCSI connected SAN or Network Attached Storage (NAS)). Then VMware vStorage VMFS allows multiple installations of VMware vSphere to access the same virtual machine files concurrently.

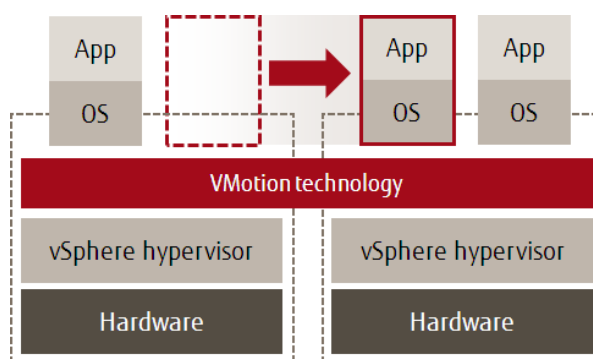
Secondly, the active memory and precise execution state of the virtual machine is rapidly transferred over a high-speed network. This lets the running virtual machine switch almost instantaneously from the source vSphere host to the destination vSphere host. Users do not notice. vMotion enables fast switchover by keeping track of on-going memory transactions using a bitmap. Once it has copied the entire memory and system state to the target vSphere host, vMotion suspends the source virtual machine, copies the bitmap to the target vSphere host, and resumes the virtual machine on the target vSphere host. Using a separate Gigabit Ethernet a vMotion process takes a few minutes.

Thirdly, the underlying vSphere host virtualizes the networks use by the virtual machine. This ensures that even after migration, the network identity and network connections of the virtual machine are preserved. vMotion manages the virtual Media Access Control (MAC) address as part of this process. Once it has activated the destination machine, vMotion simply pings the network router to ensure it is aware of the new physical location of the virtual MAC address. Since the migration of the virtual machine using vMotion preserves the precise execution state, network identity, and active network connections, the result is zero downtime and no user disruption.

User benefits

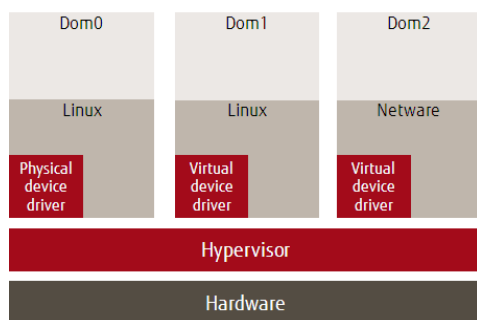
vMotion enables live migration of virtual machines between physical servers with zero downtime. This means service continuity and complete transaction integrity. vMotion becomes a key enabling technology for creating dynamic, automated, and self-optimizing datacenter. Administrators can also move planned server downtime from weekends back into normal business hours without impact on applications or users. This helps reduce administration and maintenance costs. Today over 40% of hypervisor users benefit from this live migration technology. User benefits can be summarized as:

- Optimized workloads
- Ability to perform maintenance during normal working hours, without costly out-of-hours overtime
- No negative impact on performance



2. Citrix XenServer

Xen was the Linux community's contribution to virtualization. But first, it is worth looking at how this technology is offered to the marketplace. Xen was the Linux community's contribution to virtualization. Developed at Cambridge university the base of the product is available under the familiar rules of the open source community. XenSource, a company founded by developers from that university, then took charge of further hypervisor development. XenSource also provide a charged for Xen distribution version of its own with far more functionality than the original. All major Linux vendors (and more recently ISVs like Oracle) have also developed their own derivatives based on the open source Xen version. Each licenses their product using a different model. Citrix acquired XenSource in 2008 and now develops Xen as part of its server and desktop virtualization strategy. This acquisition also resulted in a dampening effect on the uptake of the free versions. The figure below shows the basic mode of operation of a Xen hypervisor



Dom0 – Management domain for Xen guests

- Controls compute resources dynamically (e.g. memory, CPU, I/O)
- Provides interfaces to the physical server
- Provides administration tools and interfaces

Dom1,2, etc. – Guest OS

- Hosts the application workloads
- Typically uses virtual device drivers to connect to the physical drivers in Dom0 by the hypervisor
- Can also use physical device drivers directly
- Can be stored in a file image

Hypervisor

- Is the virtual interface to the hardware – virtualizes the hardware
- Manages conflicts caused by OS access to privileged machine instructions

As with VMware, the actual Xen hypervisor runs directly on the hardware. Unlike VMware however, the hypervisor does not handle the “important” functions. These are handled by what is termed “domain 0.” This privileged virtual machine runs the standard OS of the particular Linux vendor. The OS then controls each virtual machine (called in this case domain 1, 2, to domain n). Domain 0 is especially important for I/O handling.

Every I/O issued, for virtual hardware from a virtual machine, is internally redirected to domain 0. I/O is then processed on the real hardware using the original drivers included in each particular Linux distribution. This lowers the costs for OEM's certifying such hypervisors. Xen supports paravirtualization and full virtualization.

XenServer features

XenServer features can be divided into four function groups:

- High performance virtual infrastructure
- Datacenter automation
- Advanced integration and management
- Citrix VMLogix

High performance virtual infrastructure

The high performance virtual infrastructure set is free and builds the main base for virtualization, including the following function set:

- XenServer hypervisor
- XenMotion
- XenCenter multi-server management
- Conversion tools

The promotion of XenServer, based on the open-source design of Xen, is as a highly reliable, available, and secure virtualization platform. The use of 64-bit architecture allows it to provide near native application performance and unmatched virtual machine density. The intuitive wizard-driven utility ensures easy server, storage, and network setup and is referred to as “Ten Minutes to Xen” in the literature. Recovery is simplified as disk snapshot and revert create periodic snapshots of both virtual machines and data. This allows recovery to a known working state after a failure. The ability to clone disk snapshots also speeds system provisioning.

XenMotion enables the movement of workloads without user interruption while the workloads remain running.

Citrix XenCenter provides all the VM monitoring, management, and general administration functions in a single interface including configuration, patch management, and virtual machine libraries. This lets ICT staff manage hundreds of virtual machines from a centralized, management console installed on any Windows desktop. Resilient Distributed Management Architecture distributes server management data across the servers in a resource pool to ensure that there is no single point of management failure. If a management server fails, any other server in the pool can take over the management role.

Conversion tools enable conversion of physical and virtual servers (P2V and/or V2V) for faster setup and migration, and makes transformation to XenServer nearly instantaneous. Included in XenServer, they can convert any physical server, desktop workload, or existing virtual machine, to a XenServer virtual machine.

Datacenter automation

Datacenter automation includes the following function set:

- Site recovery
- High availability
- Auto-restart capability
- Dynamic workload balancing
- Host power management
- Lifecycle management
- Memory optimization

Site recovery provides site-to-site disaster recovery planning and services for virtual environments. This is easy to set up and fast to recover, and provides the important ability to test disaster recovery plans to ensure they remain valid.

High availability automates the restart of virtual machines following a VM, hypervisor, or server level failure.

Auto-restart capability protects all virtualized applications and enables higher levels of business availability.

Dynamic workload balancing provides automatic balancing of virtual machines within a resource pool. This improves system utilization and increases application performance. By matching application requirements to available hardware resources, this function also places VMs on the most suitable host in the resource pool.

Host power management uses embedded hardware features to lower datacenter electricity consumption. It dynamically consolidates VMs on fewer systems and then powers off unutilized servers as demand for services reduces.

Lifecycle management provides administrator access to defined virtual environments using a predefined set of workflows. This helps reduce complexity as well as the time and cost to develop, maintain, and deliver applications.

Memory optimization shares unused server memory among the VMs on the host server. This increases workload density by enabling more virtual machines per server. It also has a cost reducing effect as well as improving application performance and protection

Advanced integration and management

Advanced integration and management includes the following function set:

- Provisioning services
- Role-based administration
- StorageLink
- Performance reporting and alerting
- Heterogeneous pools
- Live VM snapshot and revert

Provisioning services reduce storage requirements by creating a set of “golden” images. These can then be streamed to both physical and virtual servers for faster, more consistent, and reliable application deployment.

Role-based administration helps improve security, and enables delegated access, control, and use of XenServer pools. It also maintains a tiered access structure with different permission levels.

StorageLink provides integration with leading network storage platforms. This makes it easier for storage managers to leverage their existing data management tools to maintain consistent management processes in both physical and virtual environments. Key data management processes can be created from a single StorageLink interface.

Performance reporting and alerting enables instant notification with historical reporting of VM performance. This enables rapid identification and diagnosis of faults in the virtual infrastructure.

Heterogeneous pools means resource pools can contain servers with different processor types, and support XenMotion, High Availability, workload balancing, and shared storage functionality.

Live VM snapshot and revert, captures memory and disk state during a snapshot. This speeds system provisioning and ensures periodic backup.

Citrix VMLogix group

The Citrix VMLogix group includes the following function set:

- Web self-service for Citrix XenServer
- VMLogix and Citrix OpenCloud

VMLogix integrates Web Self Service, a simple web-based console, into XenServer. Web Self Service lets ICT administrators delegate individual virtual machine (VM) administration rights to application owners and enables application owners to manage the day-to-day operations of their VM's. This makes it easier for ICT teams to build, share and deploy production-like environments on-demand in both private and public clouds. It also allows migration of virtual workloads between production stages. By providing self-service access to a single pool of computing resources, cloud providers can help users reduce their capital expenditure and improve flexibility, even across diverse virtualization and cloud environments.

Citrix XenServer with Citrix VMLogix adds key lifecycle management capabilities to the Citrix OpenCloud platform. This makes it easy for cloud providers to offer infrastructure services that extend from pre-production, to staging, and then deployment, ensuring business continuity and quality assurance. VMLogix provides support for multiple virtualization platforms. This removes the barriers between on-premise and cloud, making mobility of workloads as easy as operation within a local pool.

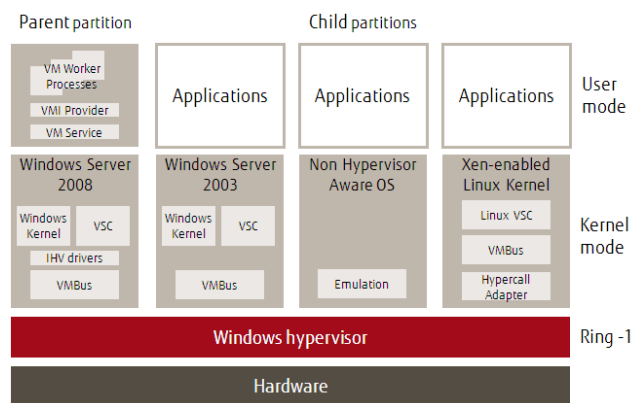
XenServer Desktop Integration

XenSource was purchased by Citrix at the beginning of 2008. As part of this, Citrix also took over the management product XenCenter. The functionality of this management product had set the standard in the Xen arena. Now Citrix has developed a new strategy around the Xen product positioning XenServer as the elementary component of this strategy.

The focus is Citrix's solution for desktop virtualization. Deep integration with XenApp Server has resulted in Citrix expanding its server-based computing portfolio to include dedicated virtualized desktops. This integration leverages, without restriction, the advantages of the well-tested ICA (Independent Computing Architecture) protocol together with all access paths and the management tools in the conventional Citrix infrastructure. At the same time, Citrix is positioning its virtualization product XenServer as the solution for virtualization of traditional Citrix Presentation Servers and Microsoft Terminal Servers. This will offer a simpler means for future scaling of these servers. Due to limitations in the Windows kernel, a single Presentation/Terminal Server instance was only able to use the capacity of new servers to a limited extent. However, with the aid of virtualization, multiple instances of such a server can now run on the same hardware. This result means a sharp increase in the number of concurrent users able to be supported. This optimization was possible only with close cooperation with Microsoft, another major vendor of virtualization technology. Citrix, as a result, is expanding its management portfolio for the Microsoft hypervisor.

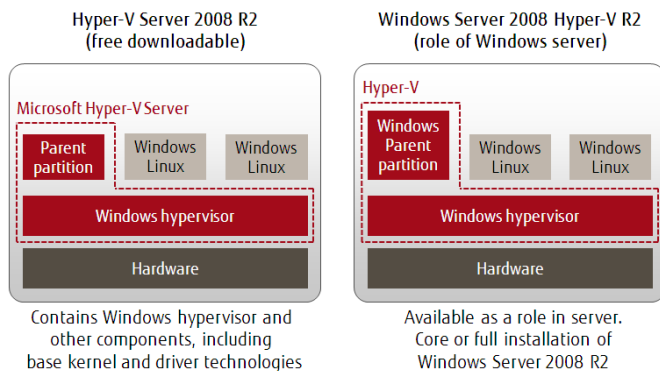
3. Microsoft Hyper-V

Microsoft released its hypervisor product in mid-2008 and provided a new version, Microsoft Hyper-V 2.0, in October 2009. Prior to 2008, Microsoft had offered Microsoft Virtual Server, a free-hosted virtual machine product that ran on top of Windows Server OS. Looking at the architecture of Hyper-V, there is some similarity to the previously explained Xen architecture:



From a naming perspective, what was domain 0 with Xen becomes the parent partition with Hyper-V. Child partitions correspond to Xen domains. One big advantage of this structure is that excellent Windows driver support automatically applies to the virtualization layer. This makes Hyper-V the server virtualization layer with the broadest driver support. In addition, Hyper-V uses all the features of the new processor families from Intel and AMD. There is optimized communication between Windows Server 2003/Windows Server 2008 and the hypervisor and physical components. Having a Windows based hypervisor and using the VMBus make this possible. Even with Linux, Hyper-V uses special hardware features from Intel (Hypercall Adapter) to improve the performance of Linux OS based applications running in Hyper-V virtual machines. This means Hyper-V, in addition to its other capabilities, fits very nicely into virtualized Linux environments.

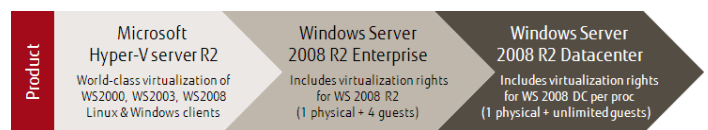
The hypervisor itself is available in two options:



Microsoft Hyper-V Server 2008 R2 is available as a free downloadable product. It enables execution of many virtual machines on a single server. In addition, key functions – like live migration and high availability – are available. Hyper-V Server 2008 R2, which runs in the parent partition, consists of the hypervisor and a basic kernel, with also includes a driver model that supports all standard drivers for Windows Server.

Hyper-V has an integrated role in the different versions of Windows Server 2008 R2. 'Server roles' are server applications that can be subsequently installed individually. In earlier versions of Microsoft Windows Server, applications such as Internet Information Services (IIS) or file release services were configured as standard when Windows Server was first installed. By contrast, Windows Server 2008 R2 cannot perform any functions by default. The administrator must first assign the required roles explicitly to the Server. Virtualization with Hyper-V is such a role.

From an operating system licensing perspective, the use of Hyper-V as a role in Windows Server 2008 R2 is often recommended. The reason is quite simple: One license of Windows Server 2008 R2 Enterprise also includes the right to run Windows Server in four virtual machines. This includes the Microsoft licenses for the four guest systems. If Hyper-V Server is used, an operating system license is required for each virtual machine. The principal rule from a cost viewpoint is: Use Windows Server 2008 R2 Datacenter (offered by Fujitsu only in the two processor version which also can be used for one processor) to run unlimited virtual machines with the Windows Server operating system on a 2 socket Fujitsu PRIMERGY server.

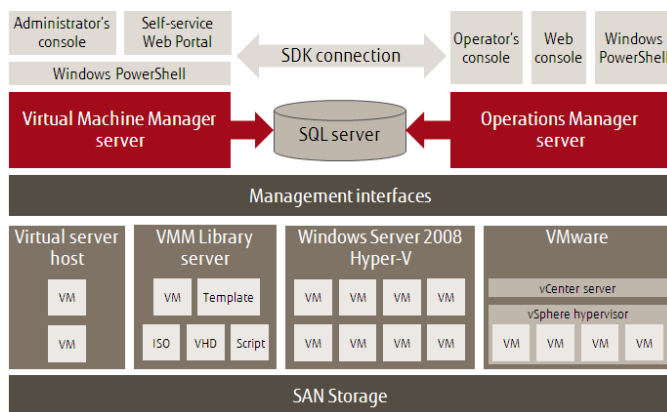


Microsoft recognized the importance of broad management around pure server virtualization technology early on. This was the reason they finished developing their management product, System Center Virtual Machine Manager (SCVMM), for virtual machines, even before the hypervisor was available.

The management of Hyper-V as a role and Hyper-V Server is identical. The included (or free downloadable) Hyper-V Management Console and Failover Cluster Manager enable execution of all functions in the virtualization layer. Moreover, the free downloadable management suite (Remote Server Administration Tool) can run on a separate PC (Windows Vista or Windows 7). This enables the same management functionality to be used remotely.

For easier and cost-effective Hyper-V virtualization management, use of SCVMM is recommended. In addition to providing the central library of the complete virtual environment, an intuitive graphic interface, and further easy to use add-on's, SCVMM is integrated with Microsoft's management products in its System Center family.

SCVMM has the following architecture:



Microsoft has included management of VMware environments in its ICT management architecture. In addition, SCVMM connects to the Operations Manager; enabling integrated management of both VMs and real instances (i.e. dedicated real servers and the real instance behind every virtualized server). The same ICT management also covers applications, whether they run on a real or a virtual machine. As a result, Microsoft has created a management solution that can administer all the resources in a modern datacenter.

Microsoft's mission is not to offer an isolated solution in the virtualized world, but rather to integrate virtualization management as a further strategic pillar in its existing comprehensive ICT management portfolio: the Microsoft System Center family. The most important System Center products in connection with virtualization are:

- System Center Virtual Machine Manager (SCVMM)
- System Center Operations Manager (SCOM)
- System Center Configuration Manager (SCCM)
- System Center Data Protection Manager (SCDPM)
- System Center Essentials (SCE, a special offering for the SME market)
- System Center Virtual Machine Manager Workgroup Edition (SCVMM WGE, a special offering for the SME market)

Today the special SME offerings are a combination of SCE (which consists of key functions from SCOM and SCCM – limited in the number of supported OS environments) and SCVMM. This is called the System Center Essentials Management Suite 2007.

This comprehensive solution enables unified proactive and efficient management of physical and virtual ICT assets. With in-built troubleshooting knowledge and simplification of the traditionally complex tasks of update management and software distribution, this solution helps to significantly reduce the standard administrative tasks. The management suite also provides functions for easy automation of standard processes and combines them with the unified management of virtual machines. SCE2010 will include further functionality (including VMM functionality) and fewer limitations in the number of OS environments supported.

Another strength of the Microsoft concept, is the development expertise at all levels of the ICT infrastructure. This includes the virtualization layer, the OS, applications, and comprehensive management of the entire environment. Microsoft can also leverage this expertise in optimally tuning its own products for this ICT infrastructure; including the gradual optimization of key applications (Office and others) for its virtualization layer. Finally, one development for the entire software infrastructure eliminates compatibility and cross product support issues that often arises when technology from different vendors is used.

In addition to standard server virtualization scenarios, Hyper-V is also well suited to desktop virtualization where XP, Vista or Windows 7 is used. Here, no explicit Windows Server CALs (Client Access Licenses) are required for the individual virtual machines – each representing a single desktop user. Instead, RDS (Remote Desktop Services) CALs are required for all desktops accessing the server.

Hyper-V also enables the execution of older versions of Windows Server OS on new server hardware; even though they are not certified with older versions of Windows Server due to Microsoft's certification policy.

It is also useful to mention that Microsoft provides a free-of-charge tool 'Disk2vhd' for simple conversion of existing physical Windows Server environments. This tool enables online migration of a running physical server onto a virtual machine. However, running this physical server in a VM does require a shutdown of the physical server and a boot of the virtual machine using the vhd-file produced during 'Disk2vhd' execution.

4. Red Hat Enterprise Virtualization (RHEV)

Red Hat started virtualization using the open source product Xen. However, following the acquisition of XenSource by Citrix, Red Hat changed its virtualization strategy. In September 2008, Red Hat announced the acquisition of Qumranet, Inc. The acquisition included Qumranet's virtualization solutions, its KVM (Kernel Virtual Machine) platform and SolidICE, a virtual desktop infrastructure (VDI). Together they provide a comprehensive virtualization platform for enterprise customers. In addition, as part of the deal, Qumranet's team of professionals who were developing, testing and supporting the solutions, (and leaders in the open source community KVM project) joined Red Hat. Red Hat subsequently focused on making the KVM technology, which is actually part of every standard Linux operating system, into its own virtualization strategy. Their approach uses kernel-based VMs. This means each VM is mapped in a normal Linux process that is managed using customary Linux mechanisms. A special KVM driver is part of the Linux kernel and, among other things, controls I/O communication between the VMs and the real hardware.

Red Hat Enterprise Virtualization for Servers is an end-to-end virtualization solution designed for pervasive datacenter virtualization. The latest Red Hat Enterprise Virtualization introduces several new features including desktop virtualization with the Red Hat Enterprise Virtualization for Desktop add-on subscription.

Overview of RHEV Hypervisor:

Red Hat Enterprise Virtualization Hypervisor is based on Kernel-Based Virtual Machine (KVM) virtualization technology, which can be deployed either as a standalone bare metal hypervisor (included), or as part of Red Hat Enterprise Linux 5 and later (purchased separately). They are installed as a hypervisor host and managed through Red Hat Enterprise Virtualization Manager for Servers

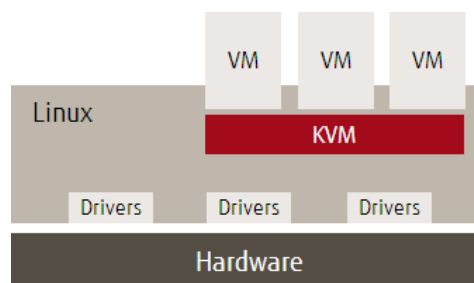
KVM is implemented as a loadable kernel module that converts the Linux kernel into a bare metal hypervisor. There are two key design principals adopted with KVM. Both have helped it develop rapidly into a stable and high performance hypervisor, enabling it to overtake other open source hypervisors.

First, as KVM was designed after the advent of hardware-assisted virtualization, it did not implement features provided by hardware. The KVM hypervisor requires Intel VT-X or AMD-V enabled CPUs and leverages those features in CPU virtualization. By requiring such hardware support KVM was able to design an optimized hypervisor solution without the "baggage" of supporting legacy hardware or requiring modifications to the guest operating system.

Secondly, KVM applied a tried and true adage – "don't reinvent the wheel". Hypervisors need many components in addition to virtualized CPU and memory. For example, a memory manager, process scheduler, I/O stack, device drivers, security manager, network stack, etc. In fact, the hypervisor is really a specialized operating system, the only difference being it runs virtual machines rather than applications. With the Linux kernel already including the core features required by a hypervisor, plus with the maturity and enterprise platform performance, from over 15 years of support and development, it was more efficient to build on that base rather than write all the same components again for the hypervisor. In this regard, KVM benefited from Red Hat's experience with Xen. One of the key challenges of Xen is the split architecture of domain0 and the Xen hypervisor. Since the Xen hypervisor provides the core platform features within the stack, it needed to implement the OS-like feature from scratch. However, because the Linux kernel was already mature and had a proven memory manager, including support for NUMA (Non-Uniform Memory Access), large-scale systems, and power management; the decision was made to incorporate the KVM into the upstream Linux kernel. Red hat submitted the KVM code to the Linux kernel community in December of 2006 and acceptance into the 2.6.20 kernel came in January of 2007. It was at this point that KVM became part of the Linux core and able to inherit all the key features in the Linux kernel.

KVM Architecture

In KVM architecture, each virtual machine is implemented as a regular Linux process, and scheduled using the standard Linux scheduler. In fact, each virtual CPU appears as a regular Linux process. This allows KVM to benefit from all the features of the Linux kernel. Device emulation is handled by a modified version of QEMU. This provides emulated BIOS, PCI bus, USB bus and a standard set of devices, including: IDE and SCSI disk controllers, network cards, and so on.



KVM supports the latest memory virtualization features from CPU vendors including Intel's Extended Page Table (EPT) and AMD's Rapid Virtualization Indexing (RVI) for reduced CPU utilization and higher throughput. Support for memory page sharing comes from a kernel feature called Kernel Same-page Merging (KSM). KSM scans the memory of each virtual machine, and VMs that have identical memory pages are merged into a single page shared between the virtual machines. If a guest attempts to change this shared page it is given its own private copy. When many virtual machines are consolidated onto a host there are many situations where memory pages can be shared – for example, unused memory within a Windows virtual machine, common DLLs, libraries, kernels or other objects common between virtual machines. Using KSM, more virtual machines can be consolidated on each host, reducing hardware costs and improving server utilization.

Hardware support

The KVM, as a part of Linux, can leverage the entire hardware ecosystem. Any hardware device supported by Linux is usable by KVM. The nature of the open source community means Linux enjoys one of the largest hardware vendor ecosystems, as new hardware adoption is rapid. This allows KVM to utilize a wide variety of hardware platforms. Without additional engineering, KVM inherits each new feature added to the Linux kernel. Ongoing tuning and optimization of Linux also immediately benefits KVM.

KVM can also store VM images on any storage supported by Linux, including IDE, SATA and SCSI local disks, Network Attached Storage (NAS) including NFS and SAMBA/CIFS or SAN via iSCSI and Fibre Channel support. Multipath I/O also improves storage throughput and provides redundancy. Again, with KVM part of the Linux kernel and support from all leading storage vendors, the KVM storage stack is also well established in production deployments worldwide.

Virtualization management

The server virtualization management system provides advanced capabilities for hosts and guests, including high availability, live migration, storage management, system scheduler, and more. Red Hat Enterprise Virtualization Manager for Servers is a feature-rich server virtualization management system that provides advanced capabilities for hosts and guests, including:

- Import and Export of Red Hat Enterprise VMs in OVF (open virtualization format)
- V2V Conversion Tools to Import Red Hat Enterprise Linux guests from Red Hat Enterprise Linux/Xen or VMware. Additional converters are expected will be available in the future
- Backup and Restore support from leading third-party backup vendors for Red Hat Enterprise Virtualization VM backup using agents in the VM
- Reporting Engine: Documented database schema and sample reports for extracting information from Red Hat Enterprise Virtualization Manager
- Live migration for movement of running virtual machines from one host to another, with no effect on performance
- Prioritized high availability where critical VMs automatically restart on a new host on hardware failure. New priority feature allows the ranking of VMs to ensure mission critical applications restart as a priority on the remaining hardware, where number of VMs may be reduced.
- Maintenance manager: It allows host upgrades and maintenance while virtual machines are running
- Image manager: It enables thin provisioning of disk storage and use of templates for fast build of new virtual machines from standard configurations
- System scheduler: It allows Red Hat Enterprise Virtualization Manager to migrate virtual machines across multiple hosts to balance workloads
- Power saver: It allows Red Hat Enterprise Virtualization Manager to consolidate virtual machines on a smaller number of hosts during non-peak hours, plus power down unneeded hosts
- Search driven user interface with tagging for searching virtual machines and host characteristics, as well as any assigned arbitrary tags
- A consistent management environment for servers and desktops

5. Oracle VM

Although Oracle entered the market quite recently, Oracle VM already delivers a large set of functions, even exceeding some of its competitors. Features like VM high availability, load balancing, live migration of virtual machines between physical servers and much more, are available. The technical basis for Oracle VM is identical to the Xen version of Red Hat; however, Oracle's implementation differs significantly in the management tools layer, service offering, integration with Oracle database, applications and middleware products.

The growing range of offerings in the market raises the question for ICT organizations of which they should consider. Should it be one for all or should it be a combination of several depending on use. At a first glance, it sounds reasonable to go for a one-for-all and follow-the-market-leader approach.

From a pure ICT infrastructure point of view, complexity and operational costs will certainly be lower by following a one-for-all approach. The main reasons for using more than one technology mainly result from price considerations. Today there are still large differences in price and functionality across the various virtual machine technologies and management tools. Oracle VM, including Oracle VM Manager, is free of charge - only service costs are charged. So adopting a one-for-all approach is typically more expensive from a purchase price point of view.

Looking at the application environment the picture may change completely. Experience has shown that not every application behaves well in a virtual machine environment. Typically, database systems and transaction-based applications have problems. This can generate significant integration costs. Another important area to consider is application vendor support. Support can be quite complex especially if several vendors are involved for hardware, OS, virtual machine technology and applications. Quite often, problems are caused by incompatibilities between different software layers and cannot be assigned to just one. That is why Oracle provides only limited or no support if Oracle software is used in virtualization environments other than Oracle VM.

Finally, there can be commercial issues when it comes to software licensing. In many ICT organizations, the complete Oracle environment is quite big, comprising many database systems, several Oracle applications and numerous deployments of Oracle middleware, including application servers. These often run on a large number of servers. Introducing virtualization to consolidate servers and to gain more flexibility in capacity usage is very appealing. However, all the potential issues regarding the technical integration of databases and applications with virtual machines, support issues, license complexity, and so on, may inhibit starting the virtualization project.

This is where the use of Oracle VM can be of great help. The complete stack, above the server hardware, all comes from the one vendor, they take responsibility for the entire support:

- OS: Oracle Enterprise Linux
- The virtualization layer: Oracle VM Server
- The virtual machine management: Oracle VM Manager, Oracle Enterprise Manager Grid Control (optional)
- Compatibility with applications, middleware and databases including tailored mechanisms for deployment
- Mix of virtualization technologies (Oracle VM at the server level with Real Application Cluster at application and database level)

Further advantage comes from the high and increasingly growing integration with higher layers of the Oracle environment. This is best illustrated by two examples:

- Oracle VM templates accelerate the deployment of a fully configured software stack by offering pre-installed and pre-configured software images. Proven configurations allow fast roll out and ongoing maintenance effort is reduced.
- Oracle Enterprise Manager proactively monitors the health of all application components, the hosts they run on, and the key business processes they support. Together with the Oracle VM Management Pack, it is now possible to manage, the virtual machines, the OS, and the software running inside the virtual machines, from a single tool.

Significant savings in integration effort, from the complete Oracle stack, well compensate for any rise in complexity from the introduction of additional virtualization technology. On the operational side, the higher productivity of the integrated stack provides management from the virtualization layer up to the application layer; this more than offsets any additional training costs.

The key strengths delivered by Oracle VM can be summarized as

- Good price-functionality ratio
- Good performance from alignment in the development of virtualization software, middleware and applications
- End-to-end support within Oracle environments
- Operational efficiency through integration of management tools

6. Novell

Novell delivers another implementation of Xen and KVM, providing users with flexibility and choice in open source virtualization hypervisors. The Xen and KVM hypervisors and comprehensive management tools ship as part of SUSE Linux Enterprise Server (SLES) at no additional cost. Using these integrated capabilities users can increase resource utilization, provision business services, and improve business continuity. SUSE Linux Enterprise Virtual Machine Driver Pack includes a paravirtualized network, plus bus and block device drivers, to run fully virtualized Windows Server and Red Hat Enterprise Linux workloads on Xen on top of SLES with near-native performance. Tight collaboration between Novell and Microsoft has resulted in optimized cross-platform virtualization – whether running Windows Server guests on SLES with Xen, or SLES guests on Windows Server with Hyper-V. Users can also run unlimited SLES guests per physical system. This is for the price of a single subscription, making it the lowest-cost operating system for virtual deployment.

As well as integrated Xen and KVM hypervisors, SLES also provides interoperability with hypervisors from Microsoft and VMware, including VMware vSphere and Microsoft Hyper-V. SLES includes a VMI-enabled (VMware's Virtual Machine Interface) kernel, for more efficient communication with VMware vSphere. This gives better performance when running as a guest operating system. Microsoft interoperability also means a more integrated set of Novell and Microsoft management tools for mixed Linux/Windows and Xen/Hyper-V environments. Optimized for x86 servers with the latest Intel multi-core architecture, SLES and the integrated open source hypervisors work well with server management software. Such combinations can be attractive in the datacenter.

Virtualization and workload management

Novell PlateSpin workload management is a portfolio of enterprise class products for physical and virtual server workload handling in mixed ICT environments. Novell PlateSpin profiles, migrates, protects and manages workloads over the network between multiple hypervisors and computing platforms. Designed to fit into existing ICT infrastructures, it is also able to scale as the datacenter evolves. With datacenter consolidation and relocation a growing strategy in overall ICT cost reduction, Novell's virtualization and workload management enables users to migrate and consolidate Windows, Linux and UNIX servers, plus VMware, Xen and Microsoft virtual machines - wherever they are located. Novell PlateSpin works well with enterprises of different sizes and help reduce costs, complexity and risk. It also helps in transforming the datacenter into a more agile, efficient and resilient ICT environment.

Server consolidation & virtualization

While many of the servers in today's datacenters are "deemed" business-critical, most enterprises are yet to embrace virtualization and migrate their workloads into a virtual environment. This is usually due to user concerns about performance issues and unplanned downtime. Novell takes a practical and safe approach to this by first collecting workload utilization data. Consolidation candidates are then identified, and consolidation scenarios are generated based on the resources needed per workload. The workload is migrated over the network onto a virtual host (P2V) or physical x86 server (P2P) and tested to ensure it runs as predicted. This has no effect on the existing production server. When satisfied, any changes that occurred during the test window can be synchronized and the new virtual workload made live. This pragmatic, three-step process presents a practical approach to proving the application will run without impact on business operations. Novell PlateSpin server consolidation technology is a good fit with large and very large enterprises looking to migrate hundreds of Windows, Linux and UNIX, business-critical workloads into a VMware, Xen, or Microsoft virtual environment.

Datacenter consolidation

Datacenter consolidation involves the planning, migration and consolidation of hundreds of servers and virtual machines. It can be an overwhelming task without the proper tools and technology. Major effort and time is required to manually identify, package, and ship existing servers and virtual hosts to a new site and then set up and rebuild those same systems. This is therefore a good time to identify and migrate underutilized servers to a consolidated virtual environment, plus migrate older servers to new and more powerful space-saving rack and blade servers.

Virtualization and workload management from Novell allows reduction in the manual effort and logistics involved in completing such site consolidation. This is done by simplifying, automating and planning the migration of servers and virtual machines over the network to a more efficient consolidated datacenter location. The solution reduces risks associated with migrating hundreds of servers and virtual machines by giving the ability to profile, migrate, and fully test the workloads in their new environments prior to going live. Such solutions can migrate hundreds of Windows, Linux and UNIX servers as well as VMware, Xen and Microsoft virtual machines.

Importantly, once user confidence grows, Novell PlateSpin datacenter consolidation supports the migration of hundreds of mixed environment servers and virtual machines across multiple datacenter locations.

Summary

VMware today is the benchmark by which all other virtualization companies are measured. It has the richest feature set, enterprise-class management tools for virtual infrastructure, and practical tools for integration into other management and hardware environments. It also has the highest market share and longest experience. It should therefore be a top pick where no other virtualization options are specifically preferred.

The Citrix strategy is an integration of XenServer with other products from their huge portfolio. Such integration offers more advanced end-to-end solutions beyond the hypervisor. In particular, it provides the longest experience and most complete set of options in desktop virtualization. If that is also a part of the virtualization equation then Citrix needs to be considered.

Microsoft's strength is in the comprehensive management that also takes care of Microsoft OSs, Microsoft applications, physical servers and server virtualization technologies other than Hyper-V. If most of the administrators are Windows trained, then Microsoft virtualization will make the cleanest and most logical addition to existing Windows environments.

Red Hat offers an end-to-end solution from KVM based server virtualization to desktop virtualization. For organizations looking to run a Linux operation or have a large proportion of Red Hat Linux environments, this comprehensive set of solutions is a very good fit.

Oracle VM is a Xen based hypervisor with specific focus on serving Oracle environments. Integrated in Oracle solutions and management tools, it will deliver the best results to reduce complexity and improve inter-operability in Oracle environments.

Novell focuses on good interoperability with other vendors (especially with Microsoft, but also VMware). It has a comprehensive systems management suite and in combination with PlateSpin technology is well positioned to provide advanced management in virtual infrastructures. In mixed environments where no particular environment dominates, Novell offers a cross platform approach that also scales well for large server consolidation task.

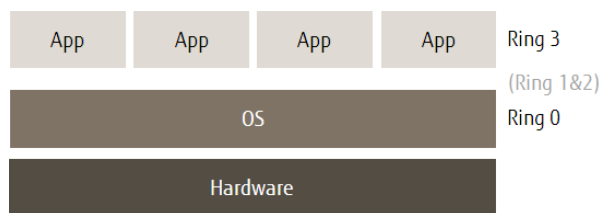
Hardware support

Optimization for hypervisors through hardware assistants

Depending on the application profile, the use of hypervisor technology could previously have a remarkably negative impact on performance. The reasons for this included simultaneous virtual address translation for multiple virtual machines and I/O emulation.

Today, these problems are being addressed by extensions to the x86 instruction set. In particular, Intel-VT and AMD-V virtualization support which now all hypervisor products support. Implementation makes hypervisors simpler, smaller, more efficient and robust. It also allows users to move more software onto new industry standard server platforms. Consequently there is no need to modify the guest OS for performance reasons, making paravirtualization less important in the future. However, it needs to be said that hardware assistants in the CPU chip will not eliminate the need for hypervisors.

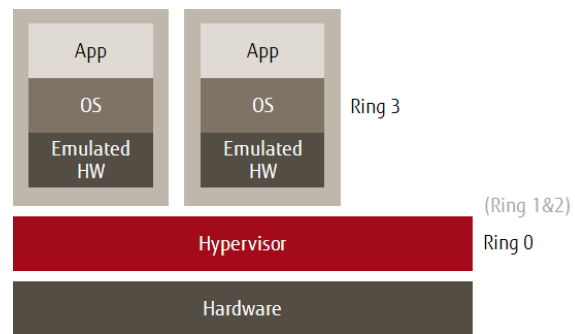
x86 operating system architecture



In this architecture, the processor provides 4 privilege levels, also known as rings. These are arranged in a hierarchical fashion from ring 0 to ring 3. Ring 0 has the most privileges, full access to the hardware, and is able to call privileged instructions.

Ring 0 is where the operating system (OS) runs with the OS kernel controlling access to the underlying hardware. Rings 1, 2 and 3 operate with lower privilege levels and are prevented from executing instructions reserved for the operating system. In common operating systems such as Linux and Windows, the operating system runs in ring 0 and the user applications run in ring 3. Rings 1 and 2 are not used by modern commercial operating systems. This architecture ensures that an application, running in ring 3, cannot make privileged system calls. However, an operating system running in ring 0 hardware does expose applications running in lower privilege levels. This model provides benefits in traditional, "bare metal" deployments, but it does present challenges in a virtualized environment.

In a virtualized environment, the hypervisor must run at the most privileged level, controlling all hardware and system functions.



In this model, the individual virtual machines then run in a lower privileged ring, typically in ring 3. However, within ring 3 we can see both virtual machines contain the OS running on virtual (emulated) hardware. Since the operating system was originally designed to run directly on the hardware, it expects to be running in ring 0 and will make privileged calls that are not permitted in ring 3. When these privileged calls are made, the hardware will trap the instructions and issue a fault - which typically destroys the virtual machine.

Much of the work performed in an x86 virtualization solution centers around handling this de-privileging of the operating system running in the virtual machine. This includes moving the OS kernel from ring 0 to ring 1 (or higher). This is sometimes referred to as "ring compression".

Binary translation

In this model, pioneered by VMware, instead of emulating the processor, the virtual machine runs directly on the CPU. Now if privilege instructions are called, the CPU issues a trap that the hypervisor can handle by emulation. However, some x86 instructions are not trapped (e.g. pushf/popf). There are also cases where the virtual machine identifies it is running in ring 3. To handle these cases, a technique called Binary Translation was developed. Here, the hypervisor scans the virtual machine memory and intercepts such calls before they are executed and dynamically rewrites the code in memory. The operating system kernel is unaware of the change and operates normally. This combination of trap-and-execute and binary translation allows any x86 operating systems to run unmodified on the hypervisor. While this approach was complex to implement it yielded significant performance gains compared to fully emulating the CPU.

Paravirtualization

While emulation and binary-translation focused on how to handle a privileged instruction executed in a virtual machine, a different approach was taken first by the open source Xen project. Instead of handling each privileged instruction as they occurred, the approach with paravirtualization modified the guest OS in the virtual machine to replace all privileged instructions with direct calls to the hypervisor. In this approach, the modified guest operating system is aware it is running on a hypervisor and can cooperate with the hypervisor for improved scheduling and I/O. It also removes the need to emulate hardware devices such as network cards and disk controllers. However, as paravirtualization requires changes to the OS, it needs to be implemented by the operating system vendor. Initially these changes were made to the Linux operating system, in the form of custom patches to the Linux kernel. Later they were incorporated into the released Linux kernel.

To use the performance benefits of paravirtualization outside the Linux community, the community developed a paravirtualization interface that supports multiple hypervisors (e.g. Microsoft Hyper-V, VMware vSphere hypervisor). Using this interface, a paravirtualized Linux operating system can run on any hypervisor that supports it. As the same guest OS kernel is able to run natively on the hardware or virtualized on any compatible hypervisor, transparent paravirtualization is achieved. This works by design, as all calls have two implementations, inline native instructions for bare hardware and indirect calls to a layer between the guest OS and hypervisor for virtual machines. Applications can be optimized for virtualization in the same way. Examples are Oracle OVM and Oracle applications or Citrix XenServer and XenApp.

Hardware assisted virtualization

Eventually, both Intel and AMD developed extensions for their x86 architecture to provide features for use by hypervisor vendors to simplify CPU virtualization. The first CPUs with these features were released in late 2005. Today most Intel and AMD CPUs include hardware virtualization support, including desktop, laptop and server product lines.

While the implementations by Intel (VT-X) and AMD (AMD-V) are different, they use a similar approach. A new operating mode is added to the CPU which now operates in either host or guest mode. The hypervisor can request a process to a CPU that operates in guest mode. While still seeing the four traditional ring/privilege levels, the CPU is instructed to trap privileged instructions and then return control to the hypervisor.

Using these new hardware features, the hypervisor no longer needs to implement the binary translation previously required to virtualize privileged instructions. VT-X and AMD-V reduced the overhead when virtualizing the CPU. However, significant resources are expended by the hypervisor when handling memory virtualization. Because the guest operating system cannot directly access memory, the hypervisor has to implement mapping between the physical host memory and the virtual memory used by the virtual machine. This is typically implemented using shadow page tables within the hypervisor.

Recently AMD developed the Rapid Virtualization Indexing (RVI) feature, previously known as nested page tables. Intel also developed the Extended Page Table (EPT) feature. Now available with the latest CPUs, they provide a virtualized memory management unit (MMU) in hardware. This delivers significant performance improvement compared to the previous software only implementations. Both Intel and AMD are continuing to add new features to their processors to improve virtualization performance, offloading more features from the hypervisor onto “the silicon” to provide improved performance and a more robust platform.

The current generation of Intel and AMD CPUs, and chipsets, are now adding support for I/O offloading. This includes secure PCI pass-through, using Intel VT-D and AMD IOMMU. This allows PCI devices on the host to be passed directly into the virtual machine. Single Root I/O virtualization (SR/IOV) further extends those features to allow special PCI devices to be split into multiple virtual PCI devices that can also be passed through to individual virtual machines. These features are allowing virtual machines to achieve the same I/O performance as the original bare metal systems.

Rigorous pursuit of this trend, by processor vendors, continues to deliver even greater agility allowing functions such as VMware vMotion and Microsoft Live Migration. This is done by:

- Reducing any loss in performance when hypervisors are used
- Enhancing the compatibility of individual processor generations

Two examples illustrate these performance improvements:

Reductions in performance loss: The AMD processor “Barcelona” has a Rapid Virtualization Indexing function that enables optimization of memory management in virtualized environments. Intel follows the same direction with its Nehalem architecture and EPT (Extended Page Tables) technology. In the past the hypervisor managed VM memory access, but now hardware tables in the processor do it. That significantly reduces the arithmetic operations in the hypervisor. VMware vSphere has already implemented all possible virtualization technology support in the hardware layer and other hypervisors will follow. Memory-intensive database applications in particular will benefit from this. Every I/O operation results in activity in the hypervisor or domain 0 (or parent partition). There the I/O operation is mapped to the real device. The same happens when the VM receives a report that an I/O operation is complete. The need for high-performance I/O handling will lead to greater future cooperation between I/O card vendors and hypervisor providers, with the aim of making VMs able to access the real hardware directly. In fact, this could be seen as a backward step, as the dependency between hardware and software reappears. However, I/O performance increases significantly. Ultimately, users will decide where their emphasis lies.

Increased flexibility: vMotion and Live Migration permit a new quality of service availability. Planned downtime, which accounts for more than 80% of downtime at a datacenter, can largely be avoided if running VMs can be moved from one system to another without service interruption. Up to now, VMs could only be moved within the same processor family or generation. This restriction forced users to build server landscapes with homogenous processors – an unacceptable requirement given the rapid development of processor technology. This problem was partially solved by cooperation between hypervisor and processor vendors. Once again, VMware was first to respond and developed its enhanced vMotion capability. Together with Intel’s VT Flex Migration and AMD-V Extended Migration technology, is now at least possible to move VMs between different processor generations from the same vendor.

Hypervisor embedded in hardware

As implemented in Fujitsu mainframes many years ago, there is now a clear trend to have virtualization as a default hardware feature. This means the hypervisor will be integrated into the server hardware, i.e. locating it in flash memory attached via internal USB. This would allow certified server hardware to be shipped ready-to-run. From server boot to running virtual machines would take just a couple of minutes. Deployment time and administration costs would also be dramatically reduced. The smaller code footprint would also further reduce the security exposure. In addition, patching and updating becomes very simple. With an embedded hypervisor, servers can be kept diskless. Embedded Hypervisors are also of particular advantage in remote locations without skilled staff. Moreover, they are the basis for appliances. Certified Fujitsu PRIMERGY servers can now be supplied with various embedded hypervisors.

State of the art

Evolution of virtual machine technology

Virtual machine technology has developed rapidly in recent years. VMware vSphere provides the best example of how users can improve flexibility and efficiency of their ICT infrastructures. VMware started with their hypervisor to address consolidation and isolation. Independence between hardware and software was also required to run old OSs on the latest hardware. Later, the focus moved to managing the virtual infrastructure leading to the VMware release of vCenter.

The objectives of these technology enhancements were as follows:

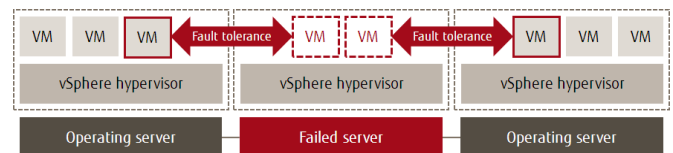
- Simple migration of physical to virtual machines
- Fast provisioning (e.g. by replication of virtual machines and flexible distribution)
- Load-balancing (improve server utilization rates and address specific resource policies with virtual machines)
- Live migration of virtual machines, including disk allocations from one physical machine to another
- Live migration of related file system entries of VMs (more flexible use of different storage units)
- Automated high availability for virtual machines (automatic restart on another server in the event of failure)
- Enhanced backup of virtual machines
- Automated patch management for hypervisor and virtual machines (even for suspended virtual machines)

Today end-to-end solutions are available. Distributed power management, can deactivate inactive components to reduce energy consumption costs. This is because most servers consume around 50% of their peak power even when idle. This also includes many different types of load balancing. The aim here is all about using the virtualized VMware vSphere farm and mapping more services onto fewer physical servers. While at the same time, ensuring that each service has its resource requirements guaranteed.

VMware Fault Tolerance (FT) is pioneering a new component that provides continuous application availability, preventing downtime and data loss in the event of server failure. Built using VMware vLockstep technology, VMware FT provides operational continuity and high levels of uptime in VMware vSphere environments. VMware FT works with existing VMware High Availability (HA) or VMware Distributed Resource Scheduler (DRS) clusters and can be simply turned on or turned off for virtual machines. When applications require operational continuity during critical period-end operations, VMware FT turns on at the click of a button to provide additional assurance. It is done by creating a running shadow instance of the primary VM, on another physical server.

The VMware vLockstep technology keeps both instances in virtual lockstep. Non-deterministic events on the primary are logged and transmitted over a gigabit Ethernet network to the shadow. As they receive identical input, both virtual machines play the exact same set of events.

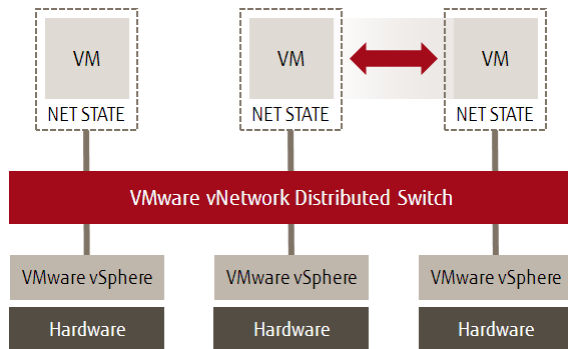
Both virtual machines access a common disk and appear as a single entity, with a single IP address and single MAC address, to other applications. Only the primary can perform writes. Both virtual machines constantly check each other's heartbeat and if the secondary loses the heartbeat of the primary, it immediately takes over. Each heartbeat is very frequent, with millisecond intervals, allowing instantaneous failover with no loss of data or status. VMware FT requires a dedicated network connection, separate from the VMware vMotion network, between the two physical servers.



Every vSphere host has its own virtual switch, which manages the network connection using the build-in LAN cards and present virtual machines. Virtualization administrators typically manage virtual machine networking at the physical server level, using virtual switches inside the hypervisor. Virtual switches require consistent configuring across many physical hosts, and aligned with the physical network. This means virtualization and network administrators must work closely together to ensure proper virtual machine connectivity. Once deployed, both must continue the close working for joint troubleshooting and monitoring of the virtualized datacenter.

For new VM's or when moving VM's from one host to another, network connections need to be adjusted. This means a lot of complex administration in large environments. VMware vNetwork Distributed Switch provides a central point of control for such datacenter-level virtual networking.

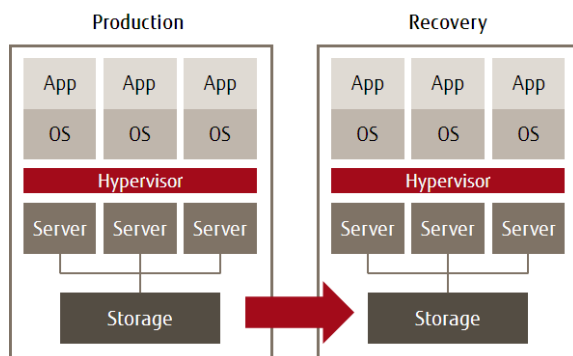
Distributed Switch spans many VMware vSphere hosts and aggregates networking at the datacenter level. VMware vNetwork Distributed Switch abstracts configuration of individual virtual switches and enables centralized administration through VMware vCenter Server. When a new host is added a standard network configuration is applied to that host. This simplifies the addition of new servers to the existing environment. Changes to virtual machine networking, across many physical servers, are also possible centrally. Many users also require that the security procedures and policies for virtual machines conform to those of physical servers for security audits.



VMware vNetwork Distributed Switch includes support for third-party virtual switches such as the Cisco Nexus 1000V virtual switch. The Cisco Nexus 1000V provides customers with virtual machine granularity and control using familiar networking tools, allowing end-to-end network management across both physical and virtual machine environments. That means that users who have installed Cisco based network environment have common and uniform network administration.

Another end-to-end solution comes with the development of VMware vCenter Site Recovery Manager (SRM). The aim here is automatic restart of the virtualized ICT infrastructure in the backup center, if the primary datacenter fails. Storage products in conjunction with vCenter SRM can now deliver a smooth, fully automated process that enables an orderly restore of the ICT operation with minimum interruption.

The mode of operation and functional range of vCenter SRM are summarized in the figure below:



- Simplified and automatic disaster recovery workflows: setup, testing, failover, and failback
- Central management of recovery plans from vCenter
- Manual recovery processes become automated recovery plans
- Simplified integration with 3rd party storage replication
- Rapid reliable, manageable, affordable, disaster recovery

It is important to understand that mirroring of the storage system is required for vCenter SRM to work.

DR for desktop virtualization is also being developed (Also refer to the separate section on desktop virtualization on page 26). This relates to the following:

- Avoidance of redundancy in provisioning OS images on expensive storage units
- New ways of delivering applications (application streaming)
- New methods of detecting viruses in centralized desktop environments.

I/O virtualization

I/O virtualization is about reducing the complexity in local area networks (LAN) and storage area networks (SAN). Servers communicate with LAN via network interface controllers (NIC) and with SAN via host bus adapters (HBA). Both types of controllers are supplied with static addresses (MAC and WWN respectively). This means that moving the OS and applications to another server, following a failure, for example, will require reconfiguration of the LAN and/or SAN.

Use of I/O virtualization will overcome these issues. MAC addresses and WWN as shown to the network must stay fixed.

However, virtualizing the operational I/O addresses will enable dynamic movement of I/O addresses between servers. If this is fully transparent to the LAN and SAN domain there is no need to change any network addresses, or create extra work for the network administrators. This I/O virtualization reduces management complexity and provides greater flexibility both when deploying new servers and services and when replacing failed servers.

Fujitsu ServerView RCVE supports two types of I/O address virtualization:

- HBA Address rename
- Fujitsu ServerView Virtual I/O Manager (VIOM) integration

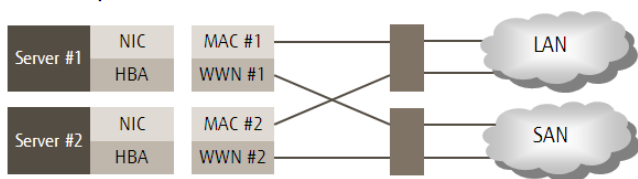
The basic idea of “HBA address rename” is the use of a “logical (virtual) WWN”, which overwrites the fixed (physical) factory-default WWN on the HBA. The logical (virtual) WWN is used to map the HBA to the system volume. This method sets the WWN of any spare server’s HBA to the same value as originally set on the production server. This allows the spare server to connect to and boot from the same boot disk used by the original production server.

Fujitsu ServerView VIOM takes care of both the virtual MAC (for NIC) and virtual WWN (for HBA) as part of the server profile assigned to each production server. If the production server fails, the WWN, MAC address, boot configuration, and network configuration are simply inherited by the spare server. Restart is then automatic using the same SAN disk previously used by the production server.

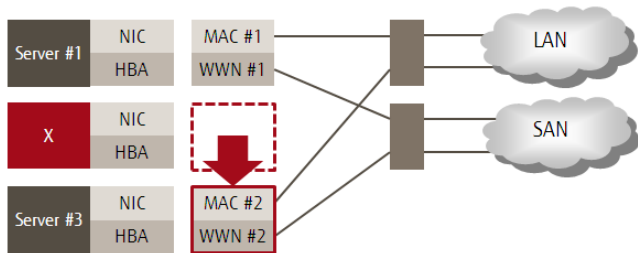
The following example illustrates this:

- Server #1 is supplied with MAC #1 and WWN #1.
- Server #2 is supplied with MAC #2 and WWN #2.
- When server #2 fails, failover to spare server #3 occurs.
- The virtual connection is “unplugged”, and both MAC #2 and WWN #2 addresses are moved to server #3. This requires no changes in any network.

Normal operation



I/O address failover



The typical benefits of this approach are:

- Separation of server management from LAN and SAN management
- Better provisioning and planning of infrastructure with less cost and administration effort
- Setup and pre-configuration of the entire LAN & SAN environment before any actual server hardware is installed
- No additional work required to change servers for maintenance or upgrades

The network and server architecture can be predefined with all necessary parameters. E.g., virtual WWN and MAC addresses can be configured in all switches. Normally network administrators have to wait until a server is delivered to acquire the right WWN or MAC addresses from their server colleagues. LAN / SAN and server administrators must then make sure that information is known to the entire ICT infrastructure. This procedure repeats every time a new server is delivered. With I/O virtualization, all server parameters for a blade system, for example, can now be configured at once. Administrators have less work to do, new servers are available earlier and the risk of human error reduces. The time required for hardware change is also decreased which results in better availability and SLAs.

Benefits:

- Flexible and fast reallocation of application (images) by moving profiles between server blades and chassis
- Automated provisioning of server resources based on user requirements
- Complete independence from OS and transparent to any application, network, or storage device

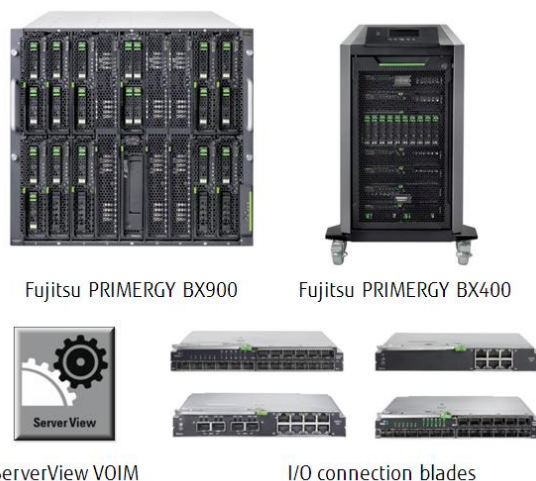
Another user requirement is the need for extra computing power at specific times - e.g. for reporting services. However, on weekends, the server normally used for production control could be used for complex reporting tasks.

The challenges are:

- Implementing the management instance for the servers and their connectors
- Assigning virtual MAC and WWN addresses to different types of LAN / SAN controllers
- Server status notification (on, off, or reboot) and re-assignment of hardware addresses

This is why I/O virtualization was done first with blade servers. The management blade (Note: Fujitsu PRIMERGY BX400 and BX900 blade servers have two redundant management blades per chassis) is the central point for collection, storage and management of each blades status. Due to the homogenous blade architecture it is easy to re-assign hardware addresses.

Fujitsu ServerView Virtual-I/O Manager provides this I/O virtualization technology for Fujitsu PRIMERGY BX400 and BX900 blade systems. The figure below shows the components required:



Desktop virtualization followed server virtualization

Up to now, virtualization concepts have mostly been applied to server environments, i.e. server OS and associated applications are the main virtualization targets. It is however equally possible to virtualize conventional PC infrastructures in a similar way. This trend is the most significant PC technology change for years. Virtual Desktop Infrastructures (VDI) enables each desktop OS to run as a virtual machine on a server in a datacenter environment. VDI matches three existing concepts: traditional desktop, traditional server-based computing, and server virtualization.

VDI gives users the best of all three of these concepts. Virtual desktops can be individualized and isolated. They also provide considerable improvements in terms of availability, security, manageability, resource utilization and energy consumption. One unique benefit of VDI is the ability gain access to a users' desktop environment from anywhere. This allows very flexible execution just by logging on at available terminal. Finally, software lifecycles can be extended, as any previous dependence between hardware and software is removed.

The addition of complementary technologies enables even greater efficiency gains. Storage capacity for virtual desktops, as well as the management of system images and applications can be reduced. The ability to run applications in isolation from the underlying hardware removes any incompatibility conflicts. Most importantly, virtual workplaces can be dynamically created, provisioned and personalized on demand, with resources only allocated when the user needs them. At the end of a user session, all resources are released for reuse. This minimizes infrastructure requirements and management effort. The result is a better quality of service level, far greater flexibility and application performance, in combination with a beneficial reduction in overall total cost of ownership.

Info box

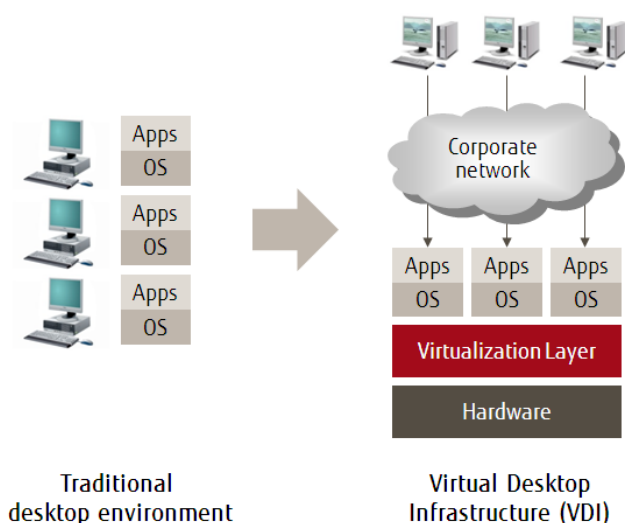
Fujitsu VDI solution

The VDI solution from Fujitsu combines the latest virtualization technologies with an integrated and complete solution stack of components. These are carefully tailored to meet each user's demands. Such an approach frees the organization from evaluating and testing all technology from scratch, which significantly lowers the barriers to adoption of new technology. End-to-end services cover consulting, design, implementation, operation and maintenance. ROI services for ICT investment decision support help determine the financial impact of infrastructure changes early in the project phase. The integrated approach means reduced project time and less risk for the organization.

Together with its full range of traditional Thin Clients, Fujitsu also provides a range of innovative Zero Clients. These provide clutter-free, space-saving productivity as well as complete silence in the office. While, the low running costs of traditional Thin Clients result from server based computing to minimize the computing power (minimal CPU, memory and graphics processing) required at the desktop; Zero Clients contain no computing power whatsoever. This revolutionary front-end device has all the benefits of Thin Clients, but further increases the manageability, security, and cost benefits, of desktop virtualization.



Fujitsu Zero Client



What is needed?

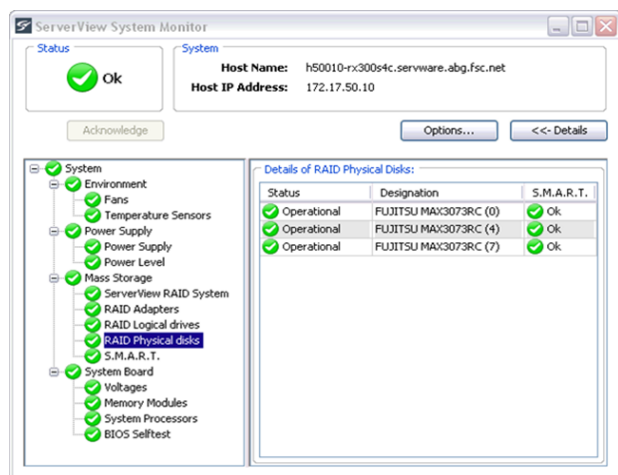
Long term coexistence of physical and virtual servers will be a reality in most datacenters

Server virtualization has become a key enabler in building more dynamic server infrastructures; allowing many users to share the vision of a flexible and more responsive ICT infrastructure. However, despite the rapid growth in server virtualization products, the percentage of x86 server workloads running in virtual machines today is still low. According to analyst reports, only 20% of all x86 server workloads currently run on virtual machines. This means, mixed operation of physical and virtual servers will be a long-term reality in most datacenters. As a result, the demand for management tools that manage both physical and virtual environments will continue.

This situation remains very complicated for many users especially with different hypervisor products in place. Taking advantage of each hypervisor's specific management tools will mean embracing further management complexity. The best advice therefore is to introduce a hypervisor-aware management tool that handles the common basic daily operations and only drop down to hypervisor specific management tools for specific functionality.

Fujitsu ServerView Operations Manager

One example is the use of a product like Fujitsu ServerView Operations Manager. VMware vSphere hypervisor supports the CIM (Common Information Model) management standard rather than SNMP. Using the new CIM provider for VMware vSphere hypervisor, Fujitsu ServerView Operations Manager can manage vSphere hypervisor -based servers much more reliably and securely than before. All-important hardware and software data are presented in identical format to data from Windows or Linux-based systems. However, Fujitsu ServerView Operations Manager automatically groups the vSphere hypervisor host and the VMs running on it to simplify administration. Fujitsu ServerView RAID Manager also supports vSphere hypervisor, and is integrated in Fujitsu ServerView Operations Manager.



Fujitsu ServerView Resource Coordinator VE (RCVE)

Dynamic server infrastructure demands wide-ranging know-how to use the necessary functionality. Administrators need to understand and manage the mix of physical and virtual servers. They also must master various virtualization technologies, as well as multi-faceted combinations of OS and hypervisors. Then of course, there is the knowledge needed to deal with network addresses, assign server resources, as well as deploy OS over SAN, and allocate predefined storage capacity to servers.

Fujitsu ServerView RCVE software was created to overcome the problems and complexity than can occur in mix infrastructures; as well as simplify overall management. RCVE standardizes the work required when administering large pools of physical and virtual servers. It helps reduce the administrative overhead by automating many processes. It also enables dynamic allocation of server resources while simplifying high availability operation.

The principle is extremely simple. Administrators define the physical and virtual resources they wish to assign to applications. Fujitsu ServerView RCVE then takes care of the rest. Administrators do not need to acquire in-depth knowledge of the new, often complex technologies involved – they just use them.

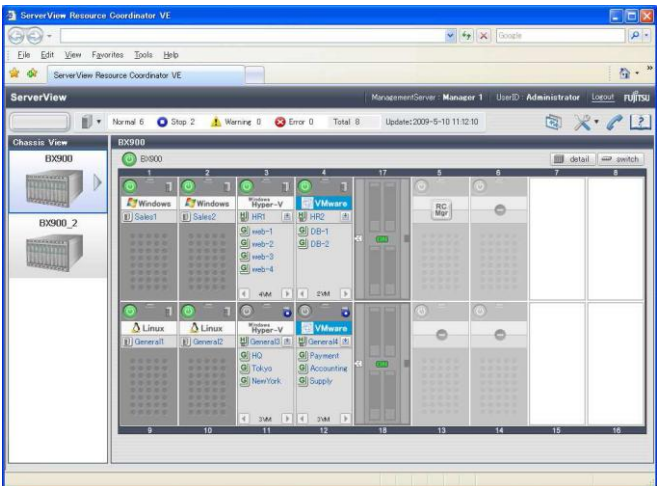
Fujitsu ServerView RCVE consolidates and simplifies administration in mixed environments and provides uniform control functions that work the same way with both physical and virtual servers. RCVE supports blade servers, rack servers, tower servers and even selected servers from 3rd-party vendors.

With virtualization, the server pool is not a static by dynamic. New servers can be added as workloads increase and new applications are rolled out. Servers can be replaced and applications relocated from one server to another as resource requirements and workloads change. To enable such rapid allocation of servers, software requires centralization. This means the OS and applications are no longer installed on physical servers, but stored as images on a central storage system. From there the appropriate image can be quickly obtained and deployed on the relevant server. It makes for very rapid assignment of new servers.

This is also true with the allocation of LAN and SAN addresses. When one server assumes the role of another, especially with blade servers, Fujitsu ServerView RCVE uses the very convenient I/O virtualization functions of Fujitsu ServerView VIOM. As a result, long system installation times needed for application relocation become a thing of the past. Applications that run on multiple servers can be cloned and then installed on the desired number of servers in a matter of minutes.

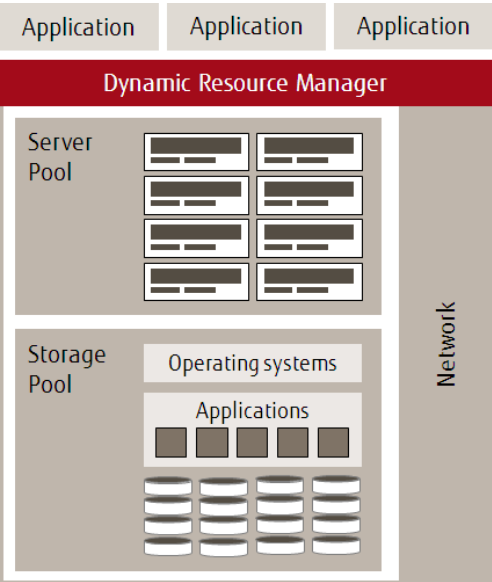
With servers only needing software images assignment, Fujitsu ServerView RCVE can also simplify server replacement. This is important for maintenance work and rollout of new software versions. With RCVE installation, rollout and replacement consumes much less time compared to conventional environments. Moreover, because both physical and virtual servers are handled in the same way, mixed environments operation is far more efficient. Day-to-day work with physical and virtual servers, even though they use different technology, can all be managed with the one set of Fujitsu ServerView RCVE tools.

If a server fails, Fujitsu ServerView RCVE automatically starts a spare system to prevent downtime. This makes it very economical to protect large numbers of production servers, as the whole pool can be protected using just one or two substitute servers (N:1 failover). This is a very cost effective alternative to standard clustering where a substitute server is required for every production server. Due to the high cost and complexity of clusters only a small portion of critical applications are typically protected. But such restrictions no longer matter in a N:1 environment. Any spare servers can be jointly used in mixed, physical and virtual environments. In addition, this efficient high availability function complements existing high availability functions provided by each hypervisor vendor for their virtual machines - and can be combined with them if necessary.



Fujitsu ServerView Resource Orchestrator (ROR)

The next step in the management of resource pools, is the pooling of physical servers or a mix of physical and virtual servers in combination with dynamic provisioning. This is the beginning of cloud computing where service virtualization is about enabling any service to run on any server. It can be achieved by storing a complete image of the software stack (OS, middleware and application) on a central storage system. Allocation of a server i.e. provisioning of the server, occurs dynamically, on demand, and just in time. This can happen when the service is needed, after a failure, or in conjunction with a change in workload. It means applications can run on servers without any fixed installation concept. The architecture of this approach is as follows:



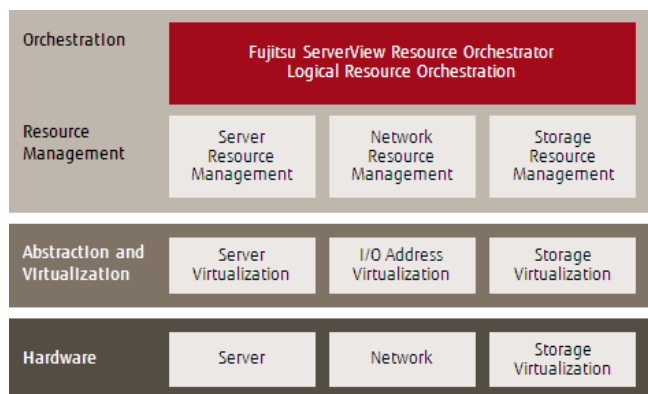
Here the key infrastructure resources, of computing, networking, storage, and the control of resources, are isolated from each other, allowing them to be independently scaled and assigned dynamically. The result is a highly adaptable infrastructure that responds to changing service needs in real time. All resources are available on demand, providing enterprise-wide agility.

Because there is only one shared OS, installation and deployment is very rapid. Software updates no longer require time-consuming software distribution. This further reduces complexity and management effort.

Fujitsu ServerView ROR enables the provisioning of system resources with just a few mouse clicks. Whether provisioning a single virtual machine or a complete server farm with both physical and virtual servers, everything is very fast. Based on the concept of cloud computing, users can obtain ICT resources on demand, without knowing where the resources are, how they are operated, or how the technology works. Fujitsu ServerView ROR is a good solution for rapid provisioning and is an enabling technology in building private and public cloud environments.

Key advantages of Fujitsu ServerView ROR compared to traditional provisioning are:

- Quick delivery of system resources to applications
- Up to 90% time saving in rollout processes
- Free up of administrative resources
- Increased use of hardware investments
- Increased quality of service
- Improved consistency and system configuration compliance through standardization and automation
- Increased agility through fast ICT infrastructure adaptation to changing business needs
- SLA-based ICT operation with high levels of service orientation
- Introduces technology necessary for building cloud environments



Fujitsu PRIMERGY BX400 and BX900 blade servers

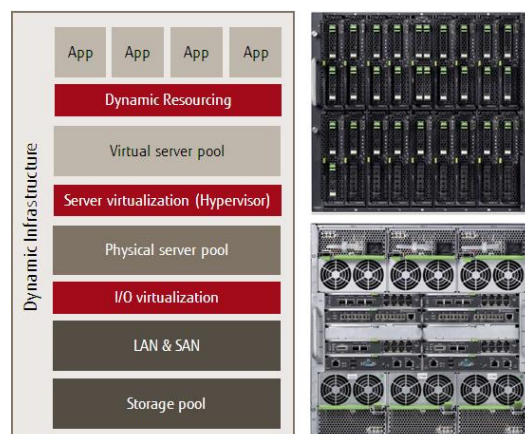
When individual servers are assigned for every application, the typical result is inefficient use of system resources and high administrative overheads. The first step in optimization therefore, is the relocation of applications from isolated servers to pooled architecture. The creation of pools and the use of server virtualization, significantly increase resource utilization and management efficiency, and reduce the server count.

The use of Fujitsu PRIMERGY BX400 and BX900 systems for pool creation makes handling of the physical servers very simple, especially as I/O connections and cables are highly consolidated. In addition, management of both physical and virtual servers is possible with just one tool – Fujitsu ServerView RCVE. There is also no need to set up separate resource pools for VMware, Hyper-V, Xen, Linux or Windows. The one consolidated resource pool rationalizes and leverages all assets. This also applies to high availability, as the N:1 failover supported by Fujitsu ServerView RCVE ensures a minimum of standby systems are required. To summarize:

- Improved utilization minimizes the number of servers required
- High availability is achieved at far lower cost
- ICT administration efficiency increases management productivity

Once the server pool is up and running, all resources become dynamic. Changes are possible within minutes. Automated operation is also possible. For example, moving server resources based on schedules (for day and night or week/weekend operation) or even in response to sudden changes in workload, becomes straightforward and automatic. The dynamic server infrastructure created by Fujitsu PRIMERGY blade servers, Fujitsu ServerView VIOM and Fujitsu ServerView RCVE make these and other scenarios simple to handle. The main additional benefits are:

- The degree of system utilization is further improved
- Resources are always available for new services at short notice
- An automatic ability to respond quickly to peak loads



Fujitsu PRIMERGY BX400 and BX900 fully complement such strategies and make virtualization and management easy as follows:

- Physical server blades are pooled by design, with full storage connection capabilities
- Complete and versatile LAN & SAN switching capability
- High performance server blades
- Memory capacity designed for virtual server pooling
- Fully certified with all major hypervisors (VMware vSphere, Citrix Xen, Microsoft Hyper-V)
- High speed mid-plane for hassle-free connectivity and fewer cables
- Fujitsu ServerView VIOM that takes away administration complexity
- Complete Scalability, plus Fujitsu ServerView RCVE and ROR, for dynamic resource orchestration

Fujitsu ETERNUS storage systems

Server virtualization as we have seen is not only a task for server hardware. Many functions like vMotion, HA, FT, DRS, SRM cannot happen without a central storage system. A storage system is the center of any VM farm. The challenge for each storage vendor is to support virtualization as best as possible. It therefore makes sense to move storage intensive tasks of the hypervisor and perform them directly in the storage system. To enable this, hypervisor vendors are delivering APIs to allow greater interaction with storage system.

For example, VMware delivers vStorage APIs that have different functions and license editions for its vSphere hypervisor.

- vStorage APIs for Data Protection
- Storage vMotion
- vStorage APIs for Multipathing
- vStorage APIs for Array Integration

vStorage APIs for Data Protection are for use by enterprise backup solutions to secure virtual machines during runtime. They allow administrators to execute scalable backup without disrupting applications or users. Fujitsu ETERNUS storage systems with vStorage APIs for Data Protection become a very effective way to enable general backup in medium to large datacenter environments.

Storage vMotion enables live migration of virtual disks from one storage location to another without disruption to users. Storage vMotion also minimizes the need to schedule application downtime required for storage maintenance. VMware Storage vMotion enables live migration of virtual machine disk files across storage arrays or operating LUNs. Now it is possible to change/extend storage systems, optimize memory I/O performance, service, or migration to another storage system, during operation.

In addition the high performance Fujitsu ETERNUS DX400/DX8000 disk storage systems support the following three functions:

- Full copy: In standard virtual machine deployment or cloning operations, data needs to be copied using vSphere servers. Now the storage systems are able to make full copies of data within the storage system environment without a vSphere server to read and write data. The result is both reduced server workloads and improved resource utilization effectiveness.
- Block zeroing: When allocating storage space to a new virtual machine, the initialization requires the writing of zeroes to fill the space. This zeroing process can now be offloaded to the disk storage systems, eliminating the need for vSphere servers to zero out large numbers of storage system blocks. This reduces server workloads and speeds up virtual machine provisioning.
- Hardware assisted locking: When exclusive data access is required, locking is now possible at the block level, as opposed to the traditional LUN levels. The result is improved VM operational effectiveness by minimization of the locking range required for access restrictions.



Conclusion

Virtualization is a game changing technology. In a world where it is now clear that every piece of information and every process will eventually be digitized, virtualization provides an opportunity to take stock and prepare for a much more computing intensive future. Importantly virtualization can deliver many short-term benefits whilst organization prepare for that future. This includes cost reductions from using virtualization to improve the use of the computing power that is already available.

Organizations will also greatly benefit from consolidating their older distributed computing environments onto fewer more powerful and more efficiently used machines. The centralization that this enables also has the potential to allow reductions in administration costs as well as improved security. Moving to a virtualized environment allows the organization to take advantage of cloud computing. That is the next logical step in virtualization and has the potential to deliver even greater economies of scale in ICT provisioning and management.

However, as with all change, the benefits need to be carefully evaluated against any possible downside. Hypervisors reduce complexity in physical environments, but also create a new complexity at the virtual level. Virtualization brings the same risk created by open systems. Open systems flexibility enabled an explosion in server deployments. The same could occur with virtual server instances, especially if strict policies are not put in place to avoid virtual server sprawl.

Each organization will need to evaluate the following:

- Management of both virtual and real resources despite the real differences in management requirements
- Applications that require special software stacks: Using different hypervisors can lead to compatibility and support problems. Examples are applications from SAP, Oracle and Microsoft. Oracle software is not certified to run on VMware for example. Analysis of hypervisor collaboration with OSs and applications, leads to complex combinations.
- The virtual machine concept is no use if an application already uses all the server resources in a native, real environment. Examples are applications with high I/O needs, such as DB servers or mail servers.
- There will be a need for additional layers of virtualization beyond the server to be fully integrated.

A major success factor will be achieving a uniform and simple management of both the real and virtual resources, with the ability to handle the complexity of virtualization easily, transparently and at an affordable cost.

Added value in server virtualization, from Fujitsu

Fujitsu is using its experience to embrace virtualization in ways that go beyond just delivering technology. It bases its approach on working with customers as partners, and ensuring that virtualization adoption integrates into the overall use and functions of the organization. It also focuses on achieving the best possible administration of the resulting ICT resources.

Fujitsu's Dynamic Infrastructures strategy, which embraces all aspects of ICT infrastructure including virtualization, follows this approach. This includes the provision of functions that take care of the new complexities of managing both physical and virtual environments in seamless and automated ways.

Fujitsu is also active in the development of cloud computing and is ideally placed to provide advice on virtualization projects with a view to cloud computing adopting in the future. Fujitsu delivers the hardware platforms, software from its own development as well as partner software, and integrates them all into complete infrastructure solutions that maximize the benefits of a virtualization approach.

The overall object is to release each organization from the need to spend too much of their own resources on designing, building, running and maintaining the ICT infrastructure. This in turn provides the ability to spend more on supporting business processes through application development and improved implementation.

Contact

FUJITSU LIMITED
Website: www.fujitsu.com
2011-03-01 WW-EN

© Copyright 2011 Fujitsu limited. Fujitsu, the Fujitsu logo are trademarks or registered trademarks of Fujitsu Limited in Japan and other countries. Other company, product and service names may be trademarks or registered trademarks of their respective owners. Technical data subject to modification and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner.